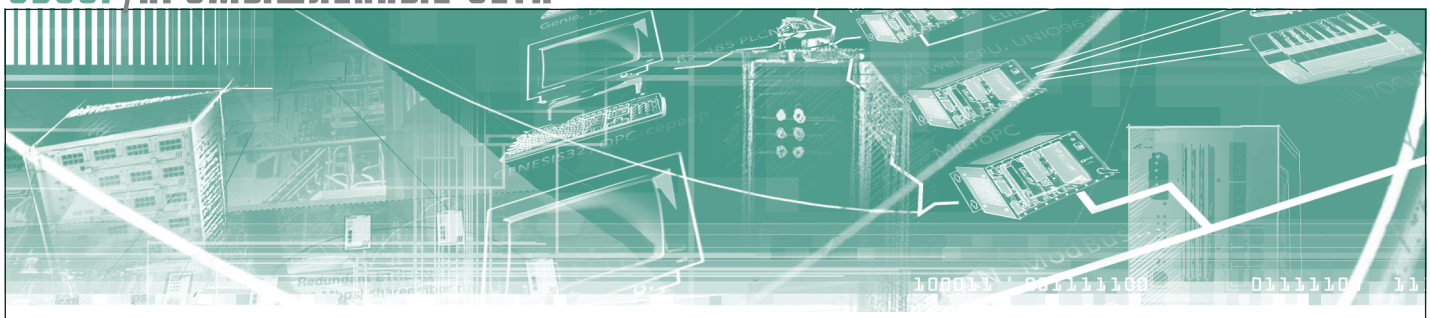


Сергей Воробьёв

“Defense in Depth” в действии. Уровень 3: защита беспроводных сетей

Данный материал продолжает цикл статей, посвящённых многоуровневой защите промышленных Ethernet-сетей на базе принципа “Defense in Depth”. В статье рассмотрены киберугрозы для беспроводных Wi-Fi-сетей, а также подходы к организации многоступенчатой защиты.

Введение

Беспроводные сети являются очень удобным и зачастую безальтернативным способом организации передачи данных. Технологии Wi-Fi, LPWAN (LoRA), ZigBee и т.д. всё чаще встречаются в самых различных сферах нашей жизни. Например, наличие Wi-Fi-сети в общественном транспорте, парках, аэропортах и т.п. воспринимается как быстрый, удобный и привычный сервис, который стал фактически частью нашей жизни.

При этом высокие скорости передачи данных (433 Мбит/с, IEEE 802.11ac), возможность увеличения расстояния передачи (до 2 км) позволяют также применить технологию Wi-Fi и на промышленных объектах. Такие гиганты мирового промышленного сегмента, как Mercedes и Volkswagen, следуя концепции Industry 4.0, уже давно и с успехом применяют беспроводные технологии передачи данных на своих заводах и предприятиях (рис. 1), существенно снижая при этом затраты на создание современной сети.

Но если рассматривать промышленные объекты в нашей стране, то ситуация не такая радужная. Доверие к медному кабелю намного выше, чем к беспроводной сети, при этом такие утверждения, что в беспроводных сетях по умолчанию используется шифрование и аутентификация, неубедительны. И наиболее частым барьером, который возникает при попытках внедрения беспроводной сети, становится организация безопасности.

Рис. 1. Пример применения беспроводной Wi-Fi-сети на промышленном объектах

То, что радиоканал передачи виден всем и его можно запросто перехватить, оказывается, как правило, финальной точкой в вопросах возможного применения. А недавняя шумиха с уязвимостью KRACK (Key Reinstallation AttaCK) взбудоражила общественность, и теперь многие просто не хотят даже думать об использовании Wi-Fi-сетей на промышленных объектах.

Но давайте разбираться более подробно в данной ситуации, ведь зарубежные промышленные предприятия не боятся и используют беспроводные технологии передачи данных, сохраняя при этом высокий уровень безопасности.

Далее рассмотрим современные подходы к обеспечению безопасности на основе принципа “Defense in Depth” в разрезе беспроводных сетей, которые предлагают гораздо больше, чем популярное шифрование данных. Приведём примеры применения такого обо-

Рис. 2. Промышленная точка доступа Wi-Fi серии OpenBAT от Hirschmann

рудования, как промышленные Wi-Fi-точки доступа серии OpenBAT компании Hirschmann с установленной операционной системой HiLCOS (рис. 2).

Беспроводная промышленная Wi-Fi-сеть: определить потребность в безопасности

Беспроводная локальная сеть передачи данных (WLAN) открывает широкий спектр новых возможностей для промышленных задач и приложений. Но в то же время неправильно либо плохо сконфигурированная система беспроводной связи в целом несёт риски для всей сети промышленного предприятия.

При конфигурировании и организации защиты сети, в том числе и беспроводной, необходимо чётко понимать, что ставится во главу угла. В первой статье данного цикла [1] мы определили, что в корпоративной среде термин «безопасность» часто приравнивается к конфиденциальности, поскольку кража информации является основной угрозой. В промышленных же сетях надёжность, доступность, целостность и подлинность данных обычно являются наиболее важными требованиями, а конфиденциальность рассматривается как несколько менее важный аспект. В то время как большинство беспроводных офисных сетей могут справляться с короткими простоями и сбоями, критически важные промышленные процессы будут к ним весьма чувствительны. В связи с этим сценарии атаки в промышленном сегменте нацелены не только на кражу паролей и данных, но и на нарушение механизмов контроля и мониторинга в производственном процессе.

Специалисты IT-сферы идут по пути отключения сети при выявлении атаки для предотвращения утечки конфиденциальной информации. Но если бы такой же подход был применён специалистами OT (Operation Techinologies), то неправильное завершение работы производственного процесса могло бы привести к более существенным последствиям. Просто взять и отключить сеть на промышленном объекте нельзя. Одним из примеров подобной кибератаки является инцидент на сталелитейном заводе в Германии в 2014 году [2]. Его суть свелась к тому, что при обнаружении атаки и аварийном завершении технологических процессов произошло нарушение связи между производственными процессами предприятия, что в итоге привело к «застыванию» доменной печи.

В итоге обеспечение безопасности Wi-Fi-сети сводится не только к защите от атак извне (кража паролей, перехват трафика), но и к организации постоянной доступности сети, чтобы свести к минимуму возможность повлиять на технологический процесс.

Оценка безопасности беспроводной сети

Чтобы разобрать возможные угрозы, которые могут существовать для беспроводной сети, необходимо рассмотреть маршрут атакующего ПК, начиная от границы сети и заканчивая ядром сети. На этом пути необходимо остановиться на возможных угрозах для промышленной сети и способах защиты. При этом одним из самых действенных методов защиты является принцип защиты в глубину – “Defense in Depth” [1], который построен на следующих подходах.

1. *Несколько уровней защиты.* Многоуровневое решение для обеспечения безопасности позволит создать разноплановую защиту. Система обеспечения кибербезопасности современного промышленного предприятия, не может полностью полагаться на одно решение, например, мощный брандмауэр, независимо от того, насколько он производительный.
2. *Дифференцированные уровни защиты.* Любая стратегия обеспечения безопасности, будь то военная, физическая или кибербезопасность, гарантирует, что каждый из уровней безопасности будет немного отличаться от других. Если злоумышленник или атакующий находит уязвимость одного уровня или барьера, то у него не должна появиться возможность преодолеть следующий уровень.
3. *Уровень защиты должен быть связан непосредственно с потенциальной угрозой.* Каждый из защитных барьеров должен быть организован, исходя из угроз. По сути, необходимо прогнозировать угрозы. Например, система может быть подвержена множеству различных угроз безопасности, начиная от компьютерных вредоносных программ и недоброжелательных сотрудников, до атак типа «отказ в обслуживании» (DoS – Denial of Service) и кражи информации. От каждой из них должна прорабатываться защита. Это позволяет использовать защиту, основанную на возможном поведении атакующих и специфике систем и протоколов. Следует также уделить внимание каждому типу угроз, опираясь на технологии и подходы, описанные далее.

Защита беспроводной сети на границе

Как было обозначено в [1], точка доступа Wi-Fi – это портал для доступа различных беспроводных устройств. При условии наличия настроек по умолчанию злоумышленник, атакующий ПК либо вредоносное ПО может провести успешную атаку на клиента, подключённого к WLAN, и на любое другое устройство в сети Ethernet.

Без надлежащей безопасности радиосигнал WLAN может быть прослушан, например, средствами свободно распространяемого дистрибутива Kali Linux, и в результате получены конфиденциальная информация и данные из сети. Атакующие могут также передать неверную информацию или управлять сообщениями в сети и мешать её работе.

При этом, в отличие от решений для проводной передачи данных, радиоканал беспроводной сети трудно ограничить и содержать в пределах какой-то определённой области. Поскольку препятствовать доступу к физической среде, радиоканалу передачи и приёма данных практически невозможно (уровни 1 и 2 эталонной модели OSI), важно, чтобы были обеспечены иные способы надёжной и безопасной работы сети на более высоких уровнях модели OSI. Необходимость защиты от подобных типов атак настолько существенна, что все текущие устройства с поддержкой WLAN обеспечивают стандартизованные процессы безопасности для установления конфиденциальности и контроля целостности в соответствии со стандартом IEEE 802.11i.

Стандарт IEEE 802.11i определяет процедуры аутентификации, шифрования и проверки данных для передачи их в WLAN. Поддержка данного стандарта обязательна в последних версиях стан-

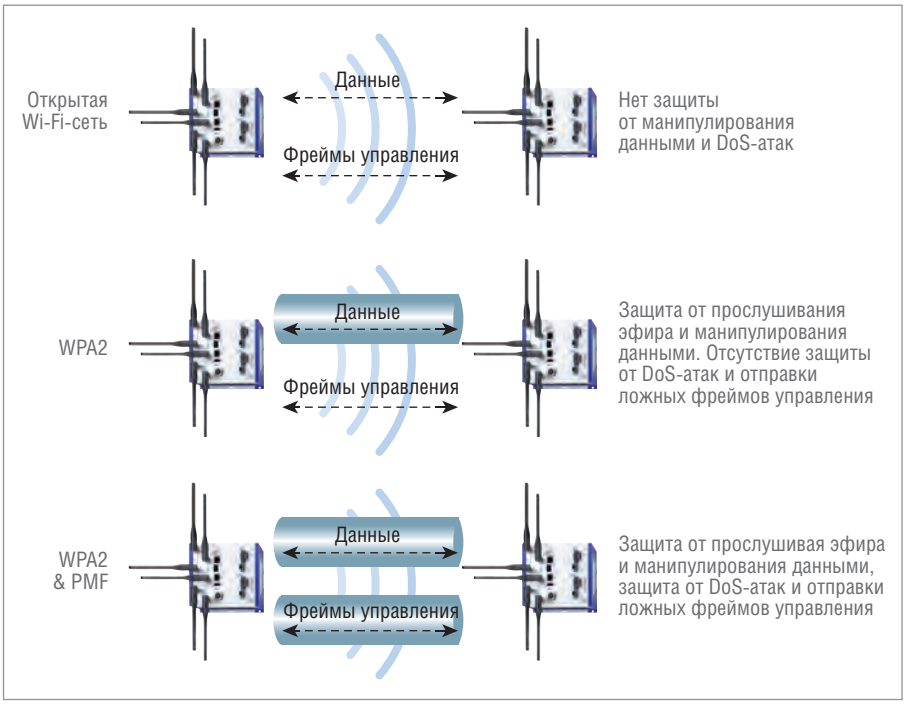


Рис. 3. Различные механизмы подключения устройств по беспроводной сети и их взаимодействие

дарта передачи по IEEE 802.11n, что требует, чтобы все текущие устройства были оснащены этой базовой защитой. Архитектура, применимая к стандарту, предусматривает индивидуальное шифрование каждой беспроводной передачи данных. Для этого между устройствами присутствуют пары ключей шифрования. Кроме того, встроенная защита целостности гарантирует, что передаваемые данные не только конфиденциальны, но и не изменяются.

Ассоциация изготовителей "Wi-Fi Alliance" интегрировала указанную архитектуру в соответствии со стандартом IEEE 802.11i в свою собственную процедуру [3], известную как Wi-Fi Protected Access (WPA2), рис. 3. Ранее используемый механизм WEP рассматривать, в принципе, не стоит.

WPA2 включает в себя два режима – Personal и Enterprise. Основное их отличие связано с механизмом аутентификации. При использовании WPA2 Personal существует один общий пароль для всех устройств в беспроводной сети (Pre-Shared Key). Этот пароль предварительно настроен для всех устройств и точек доступа. Такое упрощённое управление ключами может быть удобным лишь для очень небольших сетей.

Но для больших промышленных сетей подобное управление паролями создаёт дополнительный барьер. Ведь такие процедуры, как замена старого ключа или исключение утерянного или украденного WLAN-устройства из сети, обычно требуют ручной и сложной реконфигурации всех точек доступа и клиентов.

Для больших сетей рекомендуется использовать режим WPA2 Enterprise [4], который позволяет администратору назначать каждому устройству индивидуальный ключ и управлять ими централизованно, например, при помощи RADIUS-сервера, на котором находится база данных аутентификации.

Используя стандарт IEEE 802.1x для аутентификации на основе порта, точка доступа может проверять каждое устройство индивидуально, когда соединение установлено. Можно, например, настроить уникальный ключ для каждого устройства и управлять им в базе данных.

Таким образом, пароли могут управляться централизованно, в то время как утерянные устройства могут быть просто отключены от сети при помощи удаления соответствующих ключей из базы данных.

Кроме того, точки доступа с расширенной функциональностью позволяют отдельным устройствам назначать различные виртуальные локальные сети (VLAN) с помощью WPA2 Enterprise. Грамотная настройка VLAN позволяет увеличить общий уровень безопасности [5].

Например, беспроводной датчик и камера видеонаблюдения могут быть изолированы друг от друга путём помещения их в различные VLAN. Логически это выглядит так, что датчик взаимодействует только с сервером управления, в то время как связь камеры ограничена отправкой информации на терминал видеонаблюдения.

Пара слов про уязвимость KRACK

Осенью 2017 года мир был взбудоражен новостью, что практически все Wi-Fi-сети уязвимы и фактически любой человек, имеющий соответствующий эксплойт, может перехватить трафик и получить доступ к информации, которая ранее считалась надёжно зашифрованной. Уязвимость получила громкое название KRACK [6]. По словам исследователей, уязвимость содержится в самом стандарте WPA2, точнее, в модуле wpa_supplicant, который обеспечивает защищённое Wi-Fi-соединение по протоколу WPA/WPA2. При этом для перехвата трафика даже не надо подключаться к сети.

Как известно, беспроводные Wi-Fi-сети используют симметричное шифрование для создания основного защищённого канала передачи данных. Клиент и точка доступа знают общий ключ, который они сообщают по заведомо безопасному каналу, в Wi-Fi-сетях это пароль. Для установки соединения используется специальный механизм, состоящий из четырёх этапов (4 Way Handshake), результатом которого становится зашифрованный основной канал передачи данных. После того как соединение установлено, на каждую конкретную сессию устанавливается дополнительный согласованный сессионный ключ, который не совпадает с паролем сети, и ещё так называемое одноразовое число (nonse). Одноразовое число можно использовать только один раз за сессию. При помощи данного числа и согласованного сессионного ключа и шифруется трафик.

Особенность атаки KRACK сводится к тому, что если отправлять сообщение, содержащееся в третьем этапе установки соединения, то одноразовое число сбрасывается.

Получается, зная одноразовое число и примерное сообщение, которое будет передано по сети, можно узнать согласованный сессионный ключ соединения. А основной ключ соединения (пароль), который используется для создания защищённого канала, остаётся неизвестным. При определённых обстоятельствах и условиях атакующий может не только прослушать весь Wi-Fi-трафик сессии, но и осуществить ряд атак типа «человек посередине», когда при

помощи двух сетевых карт создаётся фиктивная точка доступа.

В итоге возникает вопрос: что делать? Как обезопасить себя и предприятие от подобного рода атак? Ответ очень прост: необходимо просто обновить прошивку. Практически все ведущие производители сетевого оборудования и популярных операционных систем уже давно выпустили обновления, которые устраняют данную уязвимость. При этом при выборе производителя беспроводного оборудования, как точек доступа, так и клиентов, необходимо уточнять периодичность выхода обновлений и скорость реакции на возможные уязвимости. Например, производитель Hirschmann выпустил обновление, устраняющее данную уязвимость, буквально через 2 недели после выхода новости. В итоге ситуацию с уязвимостью KRACK можно считать закрытой.

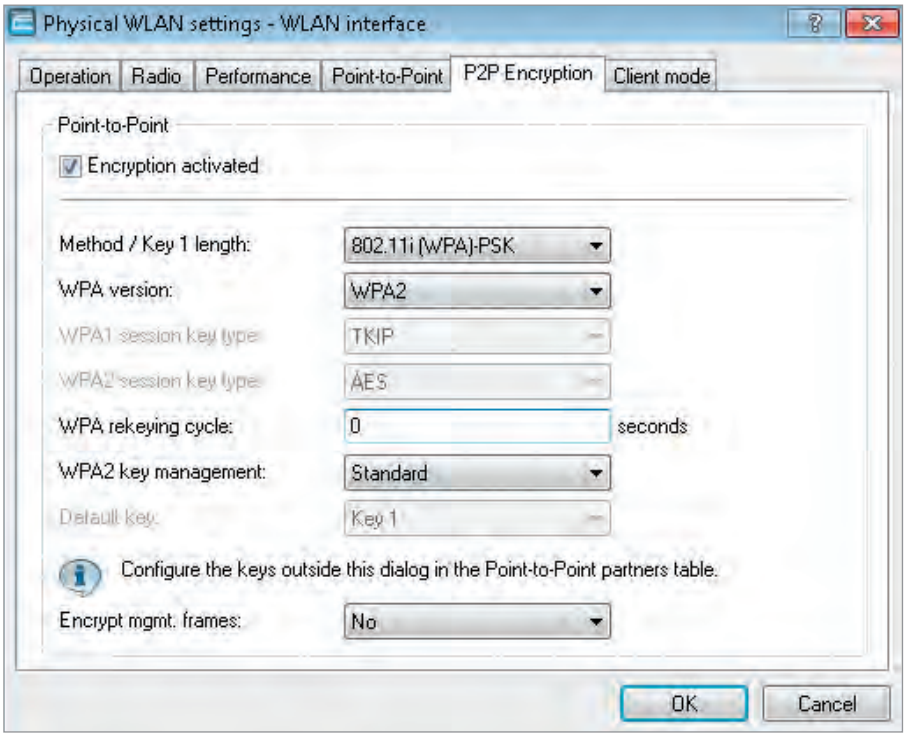


Рис. 4. Графический интерфейс настройки процедур аутентификации, шифрования и проверки данных для устройств Hirschmann OpenBAT

Повышаем надёжность и доступность беспроводной сети

В дополнение к защите границы промышленной беспроводной сети и обеспечения конфиденциальности передаваемых данных надёжность и доступность играют чрезвычайно важную роль в промышленных сетях [1]. Описанные в статье IEEE 802.11i и WPA2 предлагают механизм защиты передаваемых данных, но они не обеспечивают достаточный уровень надёжности и доступности. Функции управления сетью, которые контролируются специализированными фреймами управления, особенно уязвимы для прослушивания и дальнейшей возможности передачи ложных данных. Фреймы управления – это специализированные, чаще всего открытые служебные данные, которые передаются по беспроводной сети и служат для организации внутренней работы сети. Например, устройства могут использовать фреймы управления для входа в сеть (аутентификации) и выхода из неё (деаутентификации), инициировать новые обмены ключами и сообщать, когда происходит переключение от одной точки доступа к другой. К сожалению, защита WPA2 не включает шифрование или подтверждение подлинности для фреймов управления. Таким образом, информация о сети может быть получена из прослушиваемых фреймов, а ложные данные могут быть с лёгкостью отправлены с целью нарушить работу сети.

Одним из примеров может служить отправка сообщения для отключения клиента от беспроводной сети. Поскольку точка доступа не имеет инструментария обнаружения подлинности фреймов управления, она попросту отключит клиента от беспроводной сети. Это может создать серьёзные проблемы для промышленных предприятий, потому что устройства отключаются, а соединения становятся неустойчивыми, что приводит к серьёзным сбоям. В худшем случае это может привести к полной потере контроля оператора над всем производственным процессом.

Чтобы нейтрализовать подобные атаки, в стандарте IEEE 802.11w был введён метод под названием «Защищённые фреймы управления» (PMF – Protected Management Frames). PMF – это функция, которая позволяет шифровать фреймы управления. Фактически механизм аутентификации и шифрования, присутствующий в WPA2, расширяется для обеспечения конфиденциальности и целостности фреймов управления. На рис. 4 представлен графический интерфейс настройки функции PMF на базе Wi-Fi-точки доступа Hirschmann OpenBAT. При настройке можно точно указать параметры.

- *No:* WLAN не поддерживает PMF. Фреймы управления не шифруются.
- *Mandatory:* интерфейс WLAN поддерживает PMF. Фреймы управления всегда шифруются. Невозможно установить соединение с клиентами WLAN, которые не поддерживают PMF.
- *Optional:* интерфейс WLAN поддерживает PMF. Фреймы управления либо зашифрованы, либо не зашифрованы, в зависимости от поддержки PMF клиентом.

А что происходит вокруг? Мониторинг эфира, функция WIDS

Операции и коммуникации в Ethernet-сети часто не отслеживаются. Это особенно справедливо при работе беспроводной сети, ведь многие процессы и действия на интерфейсах выполняются автоматически и полностью невидимы даже для сетевых администраторов. Эта «прозрачность» упрощает использование и работу сети, но в то же время затрудняет распознавание атак и подозрительное поведение устройств и пользователей. Это особенно актуально для промышленных сетей, которые, как правило, обеспечивают связь между оборудованием и работают автономно в течение длительных периодов времени. Отсутствие анализа и понимания событий, которые происходят в беспроводной сети, позволяет атакам оставаться незамеченными и затрудняет принятие корректирующих действий. По этой причине важно, чтобы устройства, формирующие беспроводную сеть, оперативно обнаруживали аномальные происшествия в беспроводной связи до того момента,

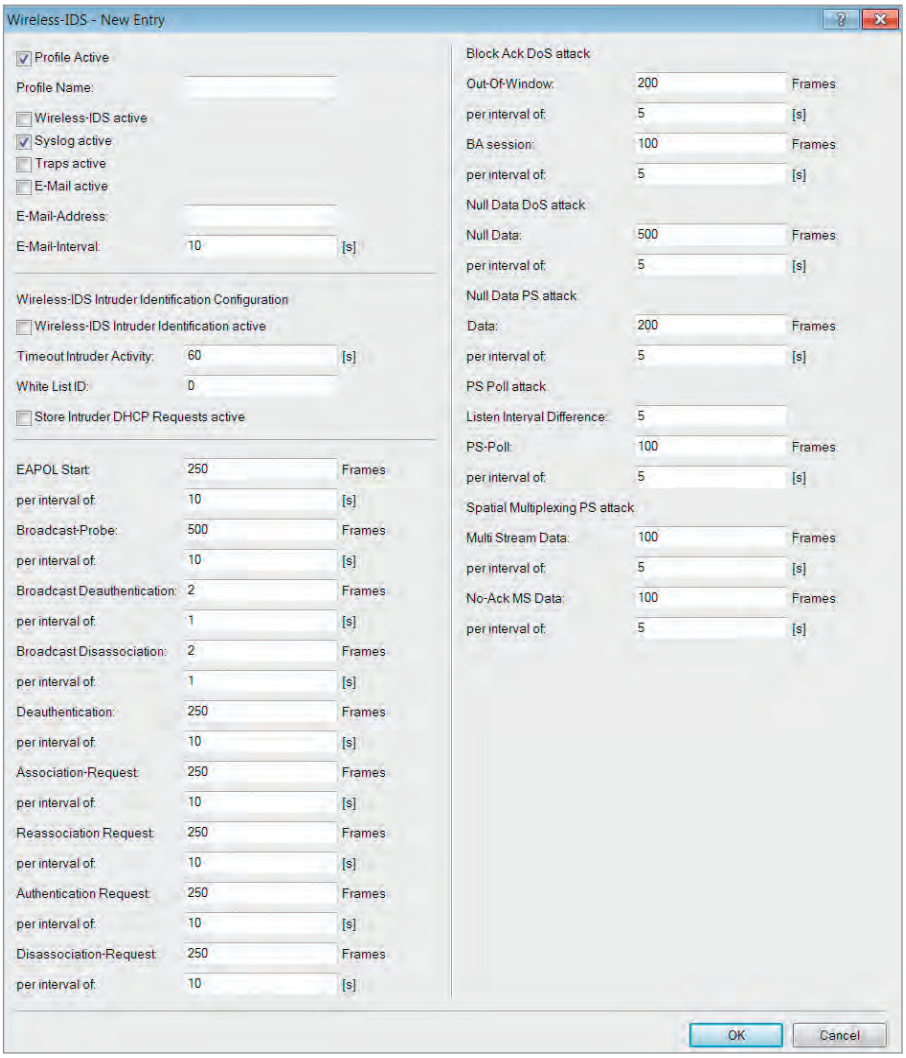


Рис. 5. Графический интерфейс настройки функции WIDS на устройстве Hirschmann OpenBAT

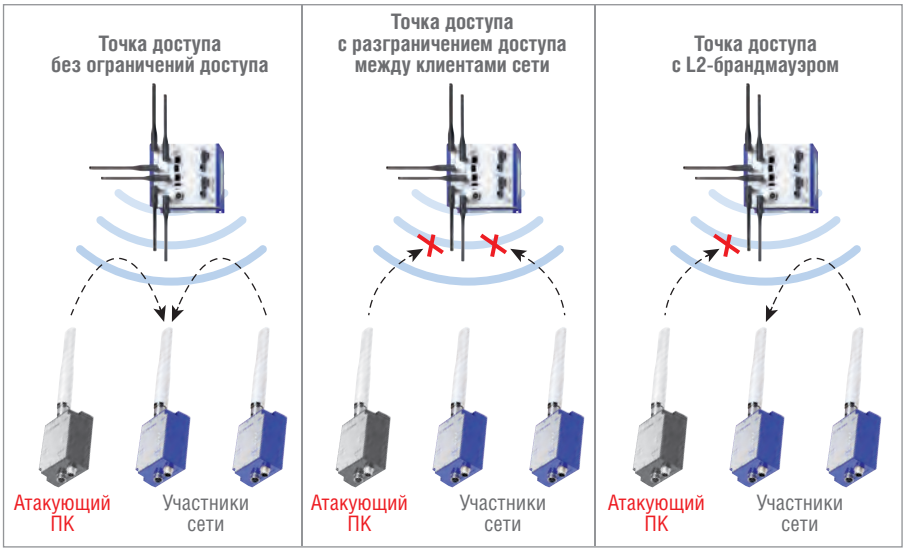


Рис. 6. Различные механизмы подключения устройств по беспроводной сети и их взаимодействие

как атакующий сможет повлиять на работу промышленного предприятия.

Подобная система имеет аббревиатуру WIDS (Wireless Intrusion Detection System). Она функционирует непосредственно в точке доступа и помогает обнаружить подозрительное поведение участников сети. Например, производится ли сейчас сканирование или приходят ли ложные фреймы управления и сообщения аутентификации. При этом WIDS регистрирует подозрительное поведение с помощью правил и пороговых значений и информирует пользователя по электронной почте, через сообщения системного журнала или протоколы сетевого управления SNMP. Решения типа WIDS можно либо встроить в точки доступа, либо добавить в сеть в качестве дополнительного компонента сети. Однако при выборе решения WLAN и WIDS необходимо учитывать экономические аспекты. Отдельные решения WIDS обычно эффективны только для крупных сетей с большим количеством точек доступа и клиентов. При проектировании небольших и средних сетей, которые часто встречаются в промышленной среде, рекомендуется использовать функцию WIDS, интегрированную непосредственно в точку доступа. На рис. 5 представлен графический интерфейс настройки данной функции на устройстве Hirschmann OpenBAT.

Ещё одним сценарием атак является подмена точки доступа под названием WiPhishing [3]. Злоумышленник, выполняющий данную атаку, устанавливает отдельную точку доступа около беспроводной сети и разворачивает новую сеть. При этом новая сеть использует идентичное наименование (SSID – Service Set Identifier). Как правило, беспроводная сеть защищена паролем, и возникает вероятность, что клиенты ошибочно подключатся к ложной беспроводной сети и передадут пароль новой точке доступа. Когда беспроводное устройство ошибочно подключено к ложной точке доступа, она, скорее всего, передаст ряд конфиденциальных данных или даже внутреннюю информацию о структуре промышленной сети.

Также возможны классические атаки типа «человек посередине», при этом они часто остаются незамеченными.

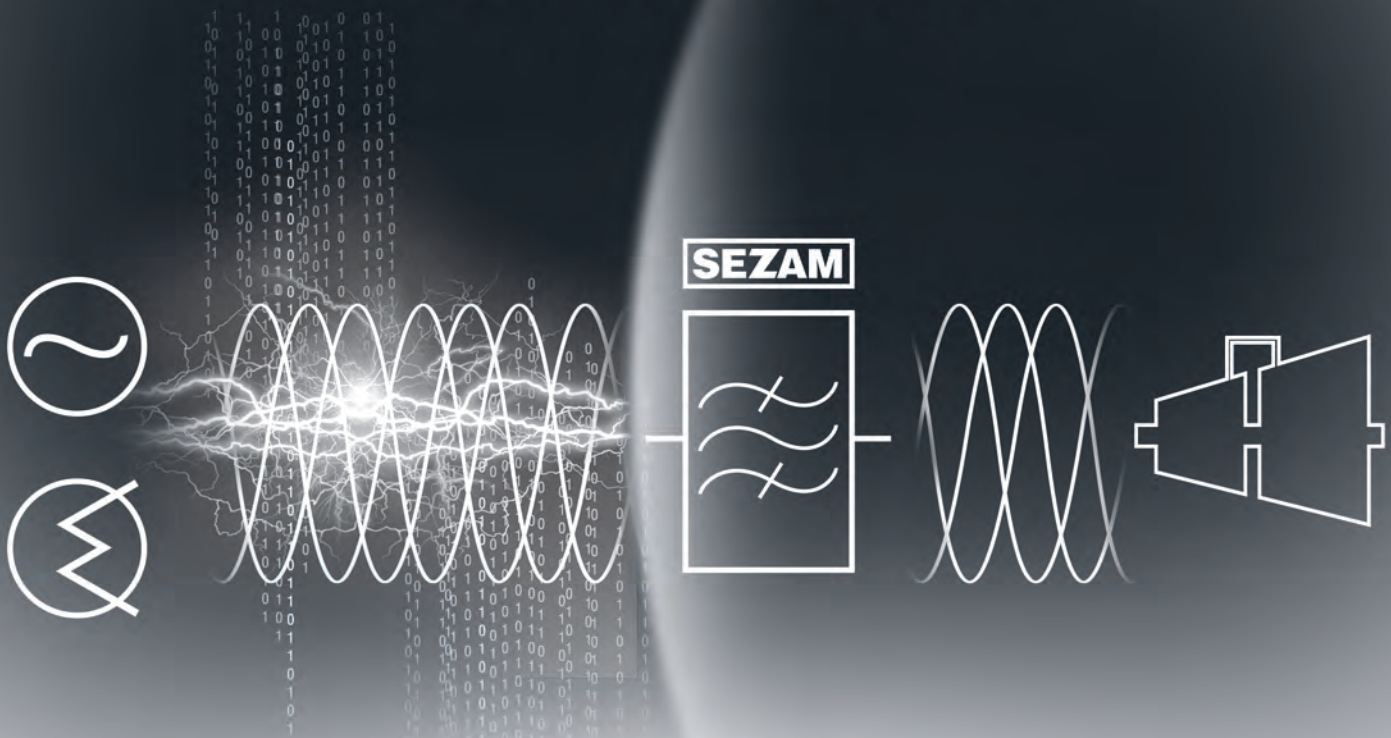
Все подобные атаки связаны с недостаточной осведомлённостью о тех процессах, которые происходят в беспроводной сети. Без её активного мониторинга окружающая среда беспроводной сети остаётся практически невидимой, пока не появятся фактические проблемы. Чтобы нейтрализовать подобные угрозы на раннем этапе, необходимо контролировать участников беспроводной сети (рис. 6). С помощью этой информации известные точки доступа в сети могут определить, использует ли неизвестное устройство SSID производственной сети или появляется новая и неизвестная точка доступа.

Проводная связь беспроводных устройств

Если рассматривать защиту только беспроводной сети, то защита не будет полноценной. Часто угрозы исходят из-

SEZAM

Там, где ИБП бессильны



Сетевой защитный модуль SEZAM

Параметры

- вход 220, 380 В
- мощность 3, 5, 10, 15 кВт
- рассеиваемая энергия импульсов перенапряжения до 20 кДж

Защита от

- повышенного напряжения
- импульсов от 4,5 до 10 кВ и разрядов молнии
- последствий обрыва нулевого провода
- преднамеренных электромагнитных воздействий

PROSOFT®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

нутри сети. Даже самое эффективное шифрование беспроводной сети не обеспечит защиту от внутренних угроз. Примерами могут служить вирусы или фишинг-атаки, когда атакующий получает доступ к сети другими способами. В соответствии с принципами "Defense in Depth" важно установить различные дополнительные барьеры, обеспечивающие многоступенчатую защиту сети.

Как только устройство-клиент подключается к беспроводной сети, оно может взаимодействовать с другими устройствами в одной сети или подсети. Это означает, что атакующий может использовать сеть для проникновения в дополнительные сетевые системы, чтобы расширить своё влияние. Эта проблема может быть решена только путём выборочного ограничения коммуникации до минимума, необходимого для запуска промышленного приложения. Как правило, точки беспроводного доступа позволяют отключать связь между всеми подключёнными устройствами, тем самым изолируя их друг от друга. Этот простой способ подавления всей возможной коммуникации «клиент–клиент» эффективно защищает все подключённые

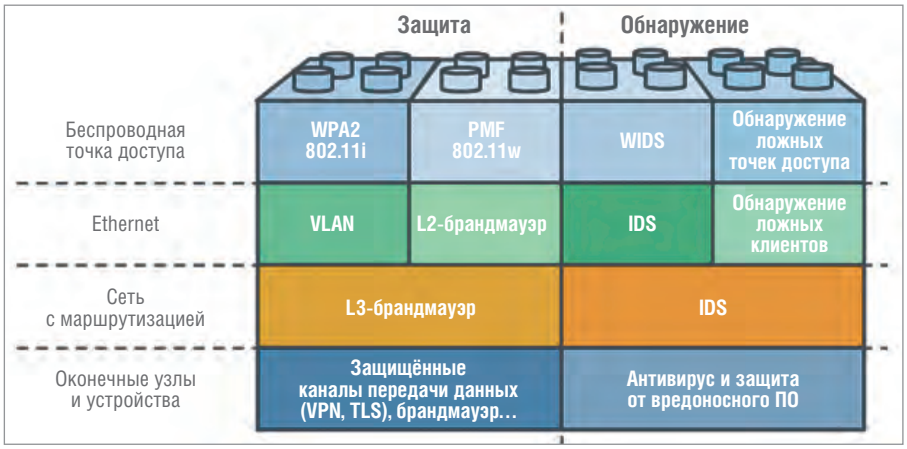


Рис. 7. Комплексная концепция защиты беспроводной сети

устройства друг от друга. Подобный подход может хорошо работать в корпоративных приложениях, а в промышленных сетях этот вариант не всегда будет оптимальным, так как может привести к дополнительной нагрузке на сеть. Например, панель управления оператора, подключённая к беспроводной Wi-Fi-сети, может напрямую связываться с беспроводным датчиком, который также подключён к той же беспроводной сети. Поэтому для сложных промышленных применений необходимо предусмотреть дополнительные барьеры, чтобы обеспечить только целевые маршруты передачи данных. Подобный механизм может быть реализован с помощью L2-брандмауэра. Это позволит выборочно фильтровать трафик между клиентами беспроводной сети и ограничить трафик между конкретными узлами или протоколами. В отличие от использования конфигурации с VLAN, брандмауэр уровня 2 является избирательным решением, поскольку позволяет разделять устройства на разные группы, где разрешена связь, а

также обеспечивает более тонкое и гибкое управление по протоколу.

Поскольку промышленные устройства часто работают в сети Ethernet без маршрутизации, важно, чтобы в сети был L2-брандмауэр, который сможет фильтровать трафик между клиентами беспроводной сети. Однако очень часто под брандмауэром понимаются решения для маршрутизируемого трафика уровня L3, который передаётся через границы сети. Брандмауэры уровня L3 позволяют передавать трафик уровня L2 и практически не защищают связь между клиентами WLAN или даже проводными клиентами в разрезе промышленной сети.

В итоге наличие в точке доступа L2-брандмауэра позволит обеспечить не только дополнительный барьер, но и лучшее сегментирование.

Защита границ сети с помощью брандмауэров в точке доступа

Промышленные объекты, как правило, распределены на большой территории. При этом они могут содержать широкий спектр взаимосвязанных приложений, сервисов и оборудования. Исходя из принципа “Defense in Depth”, отдельные участки сети промышленного предприятия должны быть изолированы друг от друга так, чтобы атакующий, который получает доступ к одной области сети, не смог повредить остальную её часть. При подобном подходе точка доступа обычно занимает центральное положение в сети, так как к ней подключаются многочисленные клиенты, представляющие собой оборудование. Из-за этого беспроводная точка доступа является отличным устройством для выборочного сегментирования и изоляции различных устройств и сетей, предоставляя функциональные возможности брандмауэра. Брандмауэр может разрешить либо запретить сетевую связь. Пакетная проверка и анализ трафика позволит ограничить связь с ненужными узлами сети, протоколами связи и даже с определённым поведением протокола.

При этом логические взаимодействия между устройствами, принадлежащими промышленному объекту, можно моделировать и применять соответствующие правила. Как и в предыдущем примере беспроводного датчика и панели управления, такое взаимодействие может также выполняться через границы сети для маршрутизируемого трафика. Структуры промышленных сетей в основном созданы непосредственно под определённую задачу и практически не меняются. Нарушения правил брандмауэра (например, если датчик внезапно начинает обмениваться сообщениями с другими системами или будет выполнять сканирование портов) становятся индикатором попытки атаки или неисправного оборудования. Нарушение правила брандмауэра может инициировать предупреждающие сообщения или электронные письма администратору, чтобы оператор сети мог быстро узнать о некорректном поведении в сети. На рис. 7 показана полная картина мер по обеспечению безопасности беспроводной сети, которая включает не только средства защиты, но и определения угроз.

Однако набор доступных средств контроля безопасности в значительной степени зависит от характера и типа конечных узлов. В некоторых случаях конечными узлами являются промышленные ПК, которые предлагают широкий спектр возможностей для повышения безопасности. В других случаях конечные точки

представляют собой встроенные системы без возможности включения дополнительных функций безопасности. Следовательно, надёжная стратегия безопасности не может опираться исключительно на безопасность только конечных узлов, но также должна обеспечивать меры безопасности на каждом уровне сети.

Пример оборудования

Описанные функции и методы существуют для всех точек доступа Hirschmann OpenBAT и программного обеспечения версии 9.0 операционной системы HiLCOS. С помощью ОС HiLCOS производитель предлагает полный набор функций для создания безопасной беспроводной сети, к которым относятся поддержка IEEE 802.11i, RADUS Authenticator и Server, IEEE 802.11w, система обнаружения вторжений в беспроводной сети (WIDS), брандмауэры уровня L2 и L3, а также обнаружение уязвимостей клиентов и точек доступа.

Эти функции могут быть развёрнуты как в небольших, так и в средних и крупных сетях без дополнительного ПО и оборудования.

Заключение

Варианты обеспечения безопасности беспроводных Wi-Fi-сетей очень разнообразны и не сводятся только к защите при помощи протокола WPA2. Согласно концепции “Defense in Depht”, для обеспечения полноценной защиты сети необходимо реализовать многоуровневую защиту. При этом комплексная организация безопасности беспроводной сети должна включать не только функциональность по защите (WPA2, PMF, VLAN, L2- и L3-брандмауэр), но и инструментарий по обнаружению различных угроз и аномалий (WIDS, IDS). Таким образом, несмотря на сложность, сочетание подобных функций в одном устройстве позволяет создать не только надёжный канал беспроводной передачи данных, но и мощный эффективный многоуровневый инструмент защиты Wi-Fi-сети от киберугроз. ●

Литература

1. Воробьёв С. Глубокая защита промышленного сетевого периметра // Современные технологии автоматизации. – 2017. – № 4.
2. Die Lage der IT-Sicherheit in Deutschland 2014 [Электронный ресурс] // Режим доступа : https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lagebe-richte.html.
3. Heer T., Wiegel B. A Construction Kit for Secure Wireless Network Design [Электронный ресурс] // Режим доступа : http://www.belden.com/docs/upload/WP00008-Construction-Kit-Wireless-Network-Design.pdf.
4. Угрозы для беспроводной корпоративной сети WPA2-Enterprise и способы защиты [Электронный ресурс] // Режим доступа : https://habrahabr.ru/company/dataline/blog/327542/.
5. Воробьёв С. “Defense in Depth” в действии. Уровень 2: защита канального уровня // Современные технологии автоматизации. – 2018. – № 1.
6. Vanhoef M. Key Reinstallation Attacks: Breaking the WPA2 Protocol [Электронный ресурс] // Режим доступа : https://www.blackhat.com/docs/eu-17/materials/eu-17-Vanhoef-Key-Reinstallation-Attacks-Breaking-The-WPA2-Protocol-wp.pdf.

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

ADLINK TECHNOLOGY INC.

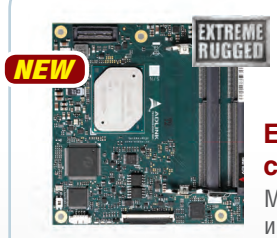
COM Express ADLINK

ДОБАВЬ МОЩНОСТИ СВОИМ РЕШЕНИЯМ

COM Express

Express-KL/KLE
cExpress-KL

Модули COM Express™ тип 6 и тип 6 Compact с процессорами 7-го поколения Intel® Core™ и Intel® Xeon P (Kaby Lake)



Express-SL/SLE
cExpress-SL

Модули COM Express™ тип 6 и тип 6 Compact с процессорами 6-го поколения Intel® Core™, Xeon™ и Celeron (Skylake)

cEpress-AL

Модули COM Express™ тип 6 Compact с процессорами Intel® Atom E3900, Pentium и Celeron, SoC

cEpress-BW

Модули COM Express™ тип 6 Compact с процессорами Intel® Pentium, Celeron N3000 и Atom x5 E8000, SoC (Braswell)

ProSoft® WWW.PROSOFT.RU
ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

МОСКВА	(495) 234-0636	info@prosoft.ru
С.-ПЕТЕРБУРГ	(812) 448-0444	info@spb.prosoft.ru
АЛМА-АТА	(727) 321-8324	sales@kz.prosoft.ru
ВОЛГОГРАД	(8442) 260-048	volgograd@prosoft.ru
ЕКАТЕРИНБУРГ	(343) 376-2820	info@prosoftsystems.ru
КАЗАНЬ	(843) 203-6020	info@kzn.prosoft.ru
КРАСНОДАР	(861) 224-9513	krasnodar@prosoft.ru
Н. НОВГОРОД	(831) 215-4084	n.novgorod@prosoft.ru
НОВОСИБИРСК	(383) 202-0960	info@nsk.prosoft.ru
ОМСК	(3812) 286-521	omsk@prosoft.ru
ПЕНЗА	(8412) 49-4971	penza@prosoft.ru
САМАРА	(846) 277-9166	info@samara.prosoft.ru
УФА	(347) 292-5216	info@ufa.prosoft.ru
ЧЕЛЯБИНСК	(351) 239-9360	chelyabinsk@prosoft.ru