ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ БЕСПРОВОДНЫХ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ (КИП)

ДЖЕФФ МЕЛРОУЗ (JEFF MELROSE)

Для обеспечения безопасности беспроводной контрольно-измерительной аппаратуры и других устройств полевого уровня используют только протоколы шифрования. Достаточно ли этого?

В последнее десятилетие наблюдается огромный рост в использовании беспроводных технологических контрольно-измерительных приборов (КИП) и других устройств полевого (низшего) уровня, поскольку беспроводные технологии предлагают существенные преимущества при развертывании такой аппаратуры, особенно в сложных условиях, где использовать обычные кабели непрактично или невозможно. Большинство поставщиков и конечных пользователей остановили свой выбор на протоколе стандарта ISA100.11a (IEC 62734) или на WirelessHART (IEC 62591). Эти два протокола во многом схожи, в том числе в части использования радиоканалов согласно требованиям стандарта IEEE 802.15.4, который определяет физический слой и управление доступом к среде для беспроводных персональных сетей с низким уровнем скорости. Однако имеющиеся в этих протоколах различия делают их несовместимыми.

В то же время более консервативные пользователи не были в полной мере убеждены в том, что устройства, зависящие от связи по радиоканалу вместо прямого проводного подключения, могут быть достаточно надежными и безопасными. В конце концов, распространение сигнала радиоволн может быть нарушено различными способами, и сама его природа накладывает на него ограничения в части путей распространения. Проблема кибербезопасности заставляет задуматься, насколько разумно иметь такие устройства и использовать радиосвязь в критически важных приложениях.

СВЯЗЬ С КРИПТОГРАФИЧЕСКОЙ ЗАЩИТОЙ ИНФОРМАЦИИ

В ISA100.11a и WirelessHART используются сложные методы шифрования, включая 128-битный симметричный алгоритм блочного шифрования, известный как Advanced Encryption Standard (AES). Но может ли он полностью обеспечить безопасность? Для целей этого обсуждения мы сосредоточим свое внимание на протоколе стандарта ISA100.11a.

> Шифрование необходимо для обеспечения безопасности беспроводных сетей, но само по себе оно недостаточно для обеспечения полной их безопасности.

«Промышленный стандарт по безопасности беспроводных каналов передачи информации ISA100 работает на двух уровнях — на транспортном и канальном, — говорится на вебсайте института по изучению проблем безопасности беспроводных коммуникаций ISA100 Wireless Compliance Institute (рис. 1). — Транспортный уровень безопасности защищает ваши данные. Он обеспечивает при их передаче из конца в конец гарантию того, что критически важные сообщения будут переданы безошибочно и безопасно. Канальный уровень защищает сеть. Он обеспечивает межузловую hop-by-hop (буквально — «при перепрыгивании от узла к узлу») гарантию того, что каждое сообщение с одного узла передано без искажений на следующий узел, с детальной диагностикой и выполнением требований по обеспечению безопасности, аккумулированных в каждом транзитном узле».

Безусловно, шифрование очень важно, поскольку без него вообще невозможно создать какую-либо безопасную беспроводную сеть. Таким образом, для всех практических целей обеспечение безопасности сразу на двух уровнях делает связь полностью криптостойкой. Этот метод не был пока еще никем взломан, и нет никаких, доступных на сегодня, известных технологий, которые в состоянии взломать его. Тем не менее, в то время как это делает механизм транспортировки данных стойким, как скала, есть много других элементов, которые вносят свой вклад в общую картину безопасности.

ИДЕНТИФИКАЦИЯ НАИБОЛЬШЕЙ УГРОЗЫ

Иметь гарантированную поддержку безопасности на транспортном уровне является, несомненно, хорошим началом, однако то, что злоумышленник сможет осуществить перехват и декодировать передаваемые данные, — не единственная угроза. Наиболее серьезной проблемой является потенциальная возможность нару-

шения радиосвязи. И осуществить это относительно легко. Рассмотрим некоторые типичные ситуации.

Посетители ряда крупных церквей в Мехико часто обнаруживают, что внутри храмов их сотовые телефоны перестают работать. Это не божественное вмешательство, а результат работы устройств, генерирующих помехи для сотовой телефонной связи. Церковные власти устанавливают такие системы («глушилки») намеренно, чтобы препятствовать ведению разговоров по мобильным телефонам.

Международная гостиничная сеть Marriott Hotels была оштрафована на $600 тыс. Федеральной комиссией по связи США (Federal Communications Commission, FCC) за блокировку бесплатных точек доступа к Wi-Fi, используемых гостями в отелях этой сети. Владельцы утверждали, что это была часть их стратегии кибербезопасности, предназначенной для защиты собственных сетей, но FCC не купилась на этот аргумент: комиссия пришла к выводу, что Marriott просто вынуждает гостей покупать их услуги в части использования Wi-Fi.

Нарушения в работе беспроводных каналов связи могут являться одной из основных причин для возникновения угрозы безопасности производственных процессов.

Компании-автоперевозчики, которые используют GPS-устройства, могут отслеживать движение своего автотранспорта. Но водители иногда покупают радиочастотные глушилки, чтобы вывести эти системы из рабочего состояния, а автомобили использовать для своих собственных нужд.

Чтобы подавить отдельные виды радиосвязи, во всех этих примерах использовались устройства для генерации помех в заданной полосе частот. Может ли это иметь место в случае с беспроводными устройствами полевого уровня? Пока нет, но никакой уверенности, что этого не сможет произойти в будущем, не существует. Уже имеются некоторые устройства, которые, скажем так, грубо, но эффективно могут нарушить связь не на каких-то конкретных частотах, а в очень широкой полосе частот. Они могут заглушить буквально все — от вещательных радиоканалов с амплитудной модуляцией до каналов связи, работающих на высоких частотах, сделав в одно мгновение связь непригодной, и для этого не потребуется нарушение шифрования. Конечная цель здесь состоит в том, чтобы вызвать отказ в обслуживании, известный как DoS (Denial of Service, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к информации либо этот доступ затруднен).

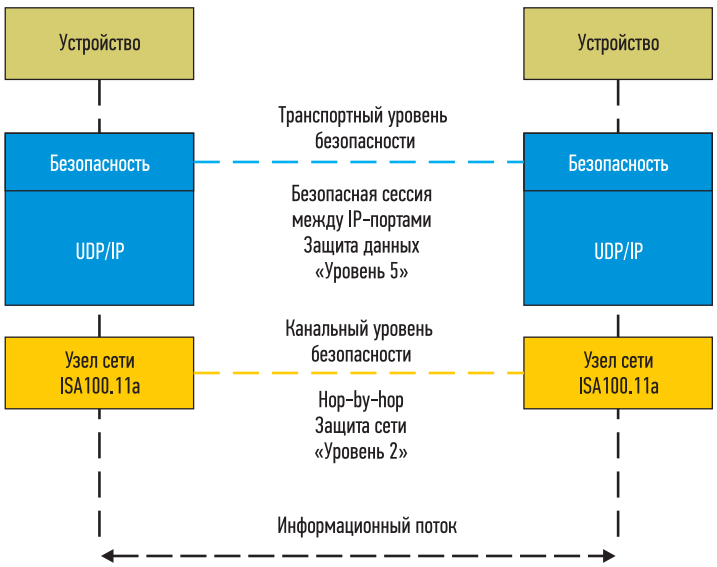


РИС. 1. ◀ Обеспечение безопасности беспроводных коммуникаций по ISA100

ОТКАЗ ИЛИ БЛОКИРОВАНИЕ КАНАЛА БЕСПРОВОДНОЙ СВЯЗИ

Если имеется возможность для DoS-атаки, является ли это поводом к отказу от беспроводных КИП? Нет, но следует всерьез задуматься о том, как их следует применять. Важно осознавать, что случится с технологическим или производственным процессом, если такой срыв в работе канала обмена данными действительно произойдет.

Устройства, предназначенные для глушения других сигналов (средства радиоэлектронного подавления), могут быть как примитивными, так и весьма сложными. Но они в любом случае должны быть расположены относительно близко к источнику сигнала, который выбран для «нападения». У таких устройств нет возможности собирать информацию или предоставлять шпионский доступ к сети. Они являются кибер-эквивалентом опасности типа «бросить камень в окно». Средство радиоэлектронного подавления нетрудно обнаружить, поэтому оно может быть быстро уничтожено.

Вмешательство, вызванное помехами, также может непреднамеренно исходить и от других источников, поэтому перебои в каналах связи не должны всегда рассматриваться исключительно как кибератака. Плохо экранированное оборудование в каком-либо месте предприятия также может стать причиной возникновения радиочастотных помех.

ХАКЕРСКАЯ АТАКА НА ПРЕДПРИЯТИЕ

Беспроводные сети имеют приоритет для хакеров, потому что они доступны для вмешательства извне, то есть из-за пределов предприятия. Человек с подходящим оборудованием может перехватывать сигнал обмена между беспроводными устройствами на уровне датчика и шлюза. Такой сигнал вполне может быть перехвачен и использован в качестве основы для атаки.

Задача хакеров — нарушить производственный процесс путем внесения в него изменений, введения заведомо неверных данных или повреждения оборудования. Еще одной их целью является кража информации.

Каковы цели хакерских атак на предприятие? Во-первых, они могут стремиться сорвать производственный процесс, например путем изменения уставок технологического процесса, ввода заведомо неправильных данных или повреждения оборудования. Компьютерный червь Stuxnet, поражавший компьютеры под управлением ОС Microsoft Windows, был примером такого подхода: его запустили с целью повредить центрифуги, использующиеся в рамках иранской ядерной программы для обогащения урана, путем изменения их эксплуатационных уставок.

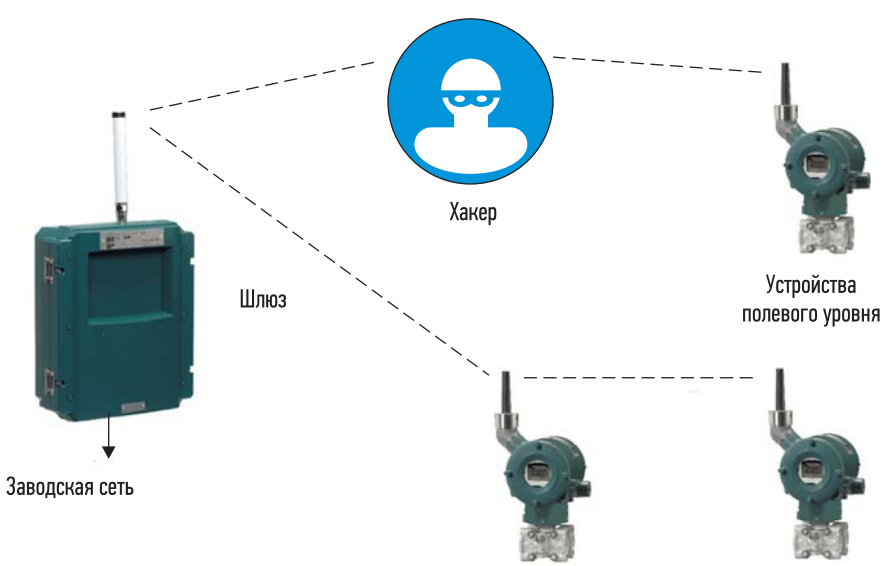
Во-вторых, целью хакеров может быть кража информации, которую потом, к примеру, можно будет продать «на сторону». Часто сети нижнего уровня (внутри предприятия) являются не так хорошо защищенными, как сети высокого уровня, поэтому хакеры могут использовать их в качестве точки входа с целью перемещения с низших уровней на верхние. Цель хакера, скорее всего, будет понятна по источнику утечки информации. Некоторые компьютерные злоумышленники делают свою работу исключительно за материальное вознаграждение, в то время как хакеры, работающие на национально-государственные структуры, могут иметь политическую подоплеку своей деятельности.

НЕЗАМЕТНОЕ ВТОРЖЕНИЕ

Хакер, намерением которого является кража информации или что-либо подобное, постарается войти в сеть незаметно и так, чтобы потом не осталось никаких следов его проникновения. Это означает, что ему нужно найти некоторую точку входа там, где есть уязвимость в обороне. Для этого необходимо провести сканирование сетей, чтобы получить всю информацию об узле, который в конечном итоге становится целью злоумышленника.

Один из способов получения доступа к беспроводной сети состоит в том, чтобы занять место узла путем перехвата связи между датчиком и шлюзом с замыканием на себя канала обмена информацией. Этот подход называется атакой типа «человек посередине» (man-in-the-middle attack — тип интернет-атак, при которых злоумышленник перехватывает канал связи, получая полный доступ к передаваемой информации). При таком способе вторжения хакер должен перехватить сигнал между двумя устройствами, а затем убедить оба этих устройства, что он и есть это другое устройство (рис. 2). В случае успеха хакер может отправить собственную информацию как «вперед», так и «назад». В результате такой атаки система управления (Distributed Control Systems, DCS) может получить, например, сообщение, что уровень жидкости в резервуаре соответствует норме, когда на самом деле уже имеет место аварийная ситуация. Хакер, таким образом, как бы становится датчиком давления (см. рис. 2) и начинает посылать свои данные в систему, либо он занимает место шлюза и начинает управлять приводом клапана, чтобы открывать или закрывать его в соответствии с инструкциями, а вернее посредством воздействия на DCS. На практике этот подход вовсе не так легко осуществить — благодаря глубокому шифрованию, о чем говорилось ранее. Более того, учитывая современные технологии киберзащиты, сделать это практически невозможно (пока). Но обеспечивает ли это безопасность сети?

РИС. 2. ▼
Атака типа «человек посередине»



УРОКИ ИСТОРИИ

Давайте ненадолго вернемся в годы Второй мировой войны. Европейские державы во главе с Германией кодировали свои стратегические сообщения, используя электромеханическую шифровальную машину под названием «Энигма» (Enigma). В ту пору эта машина казалась очень сложной, а сам процесс шифрования был реализован на таком уровне, который взломать с использованием имеющихся на то время технологий было практически невозможно. И все же союзникам удалось перехватить и расшифровать сообщения противника. Как такое стало возможным?

Дешифровщики союзников по антигитлеровской коалиции взломали не само шифрование, они вклинились в него в тот момент, когда оно использовалось. Путем склеивания элементов из захваченных кодовых книг, информации, полученной от нерадивых радистов, и путем использования умной логики они оказались в состоянии повторить действие шифровальной машины. Они смогли войти в само приложение, а не разгадать шифр. Они нашли слабые звенья в цепи и использовали их. Тем же самым путем могут пойти и современные хакеры, чтобы взломать ваши сети.

ВЗЛОМ НА УРОВНЕ ПРИЛОЖЕНИЯ

Итак, хакеры не могут нарушить шифрование, поэтому они ищут самое уязвимое место в системе. С беспроводными сетями это может привести к следующему звену в цепи безопасности, а именно — к самому приложению.

Обратите внимание на все беспроводные маршрутизаторы и шлюзы, установленные на предприятии. Являются ли они продукцией надежных и проверенных поставщиков? Известны случаи, что подобное оборудование, вполне нормально выполняющее свои функции, не обладало необходимыми возможностями в части обеспечения безопасности.

В старой технике, обладающей не очень сложной системой шифрования, хакер может найти «дыру», через которую затем проникнет в систему. Поэтому специалисты по информационной безопасности предприятия должны приложить все усилия, дабы убедиться, что такая возможность исключена.

Как настроены распознавание и идентификация ваших устройств? Однозначно ли они определяются как «ваши»? Насколько трудно хакеру будет создать новый узел в сети?

Одно из направлений атак, которое возможно осуществить через сеть, может заключаться в том, что в сеть завода будет добавлен, к примеру, новый датчик давления, способный общаться через шлюз и получить доступ к сети. Если распознавание устройства не является однозначным или не организовано должным образом, узел, созданный мошенником, может быть включен в сеть и в результате обеспечит доступ к другим этапам производства или частям завода (рис. 3). Комплексный трафик ячеистых сетей может обеспечить прикрытие для таких узлов и вызвать сложность в их обнаружении стандартными инструментами обеспечения безопасности. После создания такой опорной точки следующим шагом хакера станет переход с низкого на более высокий уровень, и далее — уровень за уровнем. Если это вторжение не заблокировать на этапе проникновения «снизу», то оно может представлять серьезную уязвимость и угрозу системе безопасности.

Системы защиты от кибератак зачастую сталкиваются с трудностями уже на нижних уровнях ячеистых сетей, использующих беспроводные устройства. Для них крайне сложно отслеживать пути передачи сигналов в круге, ограниченном обменом данными от устройства к устройству, так что атакующему нетрудно скрывать свои манипуляции, более того, у него даже имеется возможность удалять данные через сеть КИП.

ПУТИ СНИЖЕНИЯ РИСКОВ

Беспроводные сети, обслуживающие устройства полевого уровня, должны быть защищены с использованием тех же основных методов, которые применяются для проводных сетей. Различные сегменты сети должны быть разделены по соответствующим демилитаризованным зонам (Demilitarized Zones, DMZ — операционная среда между внутренним и внешним сетевыми экранами, в которой дислоцируются ПО и аппаратные средства, обеспечивающие доступ к приложениям экстрасети и предотвращающие прямое обращение к внутренней корпоративной сети) и использовать брандмауэры, чтобы ограничить движение информации из одной части сети в другую.

Не оставляйте случайных точек входа для хакеров, потому что вы можете не выключить некоторые их функции, а в их числе есть те, назначение которых вы еще не понимаете. Хакеры знают эти точки и следят за ними, а значит, вы также должны их отслеживать. Не открывайте слишком много информации о вашем оборудовании. Хакеры ищут конкретные виды оборудования и в конкретных конфигурациях, где присутствуют известные им уязвимые места. Не передавайте никому информацию о ваших сетях и о том, каким образом они настроены.

БЕСПРОВОДНЫЕ ПРИБОРЫ: ИСПОЛЬЗОВАТЬ ИЛИ НЕТ?

Беспроводные КИП и другие устройства полевого уровня дают огромные преимущества в конкретных приложениях, но важно понимать, что они также создают и новые «болезненные» точки. Да, здесь всегда есть возможность для атакующего ваше предприятие хакера внедриться и пройти через беспроводную систему. Однако в большинстве случаев злоумышленники будут искать более легкие пути для достижения своих целей, и в большинстве случаев будут пытаться найти другую уязвимость в вашей системе для использования ее в качестве точки входа.

* * *

Важный вопрос — как относиться к нарушениям в работе каналов связи? Когда все устройства установлены на свои места и работают, как будет выглядеть наихудший сценарий? Как вы будете работать, если все беспроводные устройства отключатся на некоторый период времени? Может ли это вызвать проблемы?

Если на то время, пока ситуация со сбоем в работе беспроводных КИП не будет решена, вы все еще сможете сохранять безопасное функционирование производства, нет никаких причин отказывать себе в тех преимуществах, которые может дать использование беспроводных устройств.

В любом случае, беспроводные устройства следует приобретать у проверенных поставщиков, их развертывание необходимо осуществлять надлежащим образом, с принятием всех основных мер безопасности, и не оставлять их работу без присмотра. ⬣

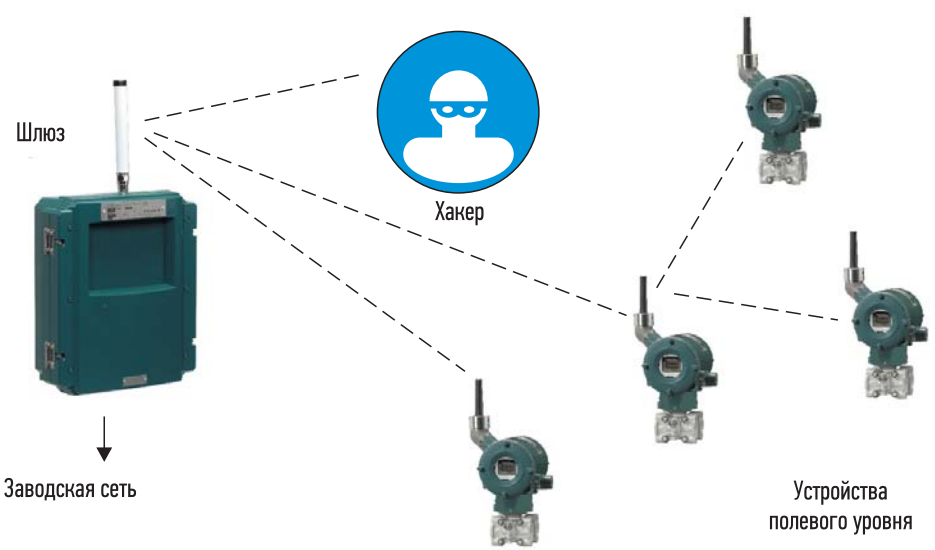


РИС. 3. ▼ Атака с помощью создания нового узла в сети