Обеспечение реальной защиты связи с помощью DECT-совместимых решений.

Plantronics предлагает гарнитуры, соответствующие стандартам DECT, и оптимизированные решения для централизованного управления.

Технология DECT (технология усовершенствованной цифровой беспроводной связи) — это технология беспроводной связи в диапазоне частот 1,9 ГГц. Использование выделенного диапазона частот позволяет обеспечить высокий уровень безопасности и качества передачи звука в производственных и бытовых условиях. DECT часто рассматривается как «помехоустойчивая технология», поскольку выделенный для нее диапазон частот не используется для других технологий, таких как Wi-Fi.

Безопасность является одним из преимуществ технологии DECT. Радиосвязь осуществляется в цифровом режиме на базе технологии множественного доступа с временным разделением (TDMA) и динамического выбора каналов с использованием более 10 несущих и 24 временных интервалов, а также многоуровневой системы безопасности. Многоуровневая система, предусматривающая подписку, шифрование и аутентификацию, обеспечивает очень высокий уровень защиты от несанкционированного прослушивания переговоров. В некоторых отраслях, таких как здравоохранение и финансы, применение решений для беспроводной связи на базе DECT позволяет обеспечить максимальную защиту и конфиденциальность.

СООТВЕТСТВИЕ ПОВЫШЕННЫМ СТАНДАРТАМ БЕЗОПАСНОСТИ DECT

Беспроводные решения на базе DECT компании Plantronics стали первыми устройствами в отрасли, соответствующими как базовым, так и повышенным стандартам обеспечения безопасности DECT, которые определены Европейским институтом стандартов по телекоммуникациям (ETSI).

Необходимость доработки стандартов DECT стала очевидной в 2009 году, когда группа «белых» хакеров, известная как DeDECTed Group, опубликовала документы, в которых были описаны уязвимости устройств DECT, соответствующих базовым стандартам. В частности, группа хакеров обнаружила возможность несанкционированного доступа в случаях, когда для устройств DECT не использовались стандартные механизмы аутентификации и шифрования, определенные в стандартах ETSI. В устройствах DECT компании Plantronics всегда использовались встроенные механизмы аутентификации и шифрования.

Результаты исследований, полученные DeDECTed Group, были рассмотрены организацией DECT Forum, в состав которой входит и компания Plantronics. По итогам рассмотрения в 2013 году была запущена официальная программа сертификации в соответствии со стандартами безопасности DECT. Данная программа предусматривает независимое тестирование и проверку устройств в сертифицированной лаборатории.

РЕШЕНИЯ КОМПАНИИ PLANTRONICS СООТВЕТСТВУЮТ ПОВЫШЕННЫМ СТАНДАРТАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ DECT

В новых стандартах DECT представлены рекомендации по улучшениям в четырех новых областях (см. ниже). При этом общее число категорий безопасности увеличивается до восьми. Фактически компания Plantronics стала первым поставщиком устройств для беспроводной связи, который обеспечил полное соответствие стандартам безопасности, определенным организацией DECT Forum: поставки гарнитур Plantronics серии CS500 с расширенными функциями обеспечения безопасности начались в октябре 2013 г.

В январе 2016 г. начались поставки гарнитур Plantronics серий Savi 400 и Savi 700 с расширенными функциями обеспечения безопасности, дополнивших набор решений DECT компании Plantronics. Во всех устройствах DECT компании Plantronics реализованы восемь функций обеспечения безопасности, определенные организацией DECT Forum:

СТАНДАРТНЫЕ ФУНКЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ DECT

1. Процедура регистрации и применение ограничений по времени для определения 64-разрядного ключа аутентификации: базовая станция остается доступной для регистрации только 120 секунд. Благодаря этому попытки регистрации гарнитуры на базовой станции могут предприниматься только в том случае, если регистрация инициируется пользователем. При этом она должна быть завершена в течение 120 секунд.
2. Инициируемая активация шифрования (на базовой станции и гарнитуре): активация шифрования поддерживается базовой станцией и гарнитурой. Шифрование активируется на базовой станции для всех вызовов. Ранее некоторые устройства DECT не обеспечивали активацию шифрования для всех вызовов.
3. Назначение ключей во время передачи: базовая станция обеспечивает создание и назначение (64-разрядного) ключа аутентификации пользователя (UAK) при регистрации гарнитуры. Это помогает исключить уязвимость базовой станции и гарнитур для атак с активным вмешательством в соединение. Ключ аутентификации используется во время связи как базовой станцией, так и гарнитурой.
4. Аутентификация гарнитуры: базовая станция обеспечивает аутентификацию гарнитуры для подтверждения ее подлинности и исключения попыток вмешательства в соединение или имитации разрешенных гарнитур. Эта функция исключает возможность установления связи между гарнитурой и базовой станцией без взаимной аутентификации.

РАСШИРЕННЫЕ ФУНКЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ DECT

5. Улучшенный генератор случайных чисел: алгоритм повышенной надежности, позволяющий избежать использования дублированных начальных чисел при генерировании ключей шифрования. Данное усовершенствование исключает возможность определения случайного числа с помощью последовательных попыток для последующего использования этого числа при создании ключей.
6. Оценка поведения участников соединения с использованием таймаута шифрования для разъединения вызова: если поведение участника соединения отличается от ожидаемого, т. е. он не инициирует шифрование в течение определенного времени, это рассматривается как попытка нарушения защиты и вызов разъединяется.

   Попытки взлома должны осуществляться абсолютно безупречно, поскольку любое взаимодействие между гарнитурой и базовой станцией, выходящее за рамки ожидаемого алгоритма, приведет к разрыву соединения.
7. Раннее шифрование: активация шифрования непосредственно после установления соединения, перед обменом какими-либо сообщениями протокола более высокого уровня, включая идентификатор вызывающего абонента, набранные цифры и т. д. Обмен информацией в незашифрованном виде не осуществляется.

DECT 101: преимущества решений DECT компании Plantronics

ПОДТВЕРЖДЕНИЕ ПОДПИСКИ
Базовая станция и удаленные устройства сопряжены друг с другом, что позволяет им легко выполнять взаимную идентификацию. Секретный ключ аутентификации вычисляется на базе стандартного алгоритма аутентификации DECT (DSAA). Полное определение этого алгоритма предоставляется только производителям оборудования. Для повышения безопасности время действия подписки устройств ограничено.

АУТЕНТИФИКАЦИЯ
На обеих сторонах соединения выполняется проверка корректности используемого ключа аутентификации и вычисление криптографических ключей (используемых для шифрования данных, передаваемых по беспроводному интерфейсу) с применением стандартного шифра DECT (DSC). Определение этого алгоритма предоставляется только производителям оборудования.

ШИФРОВАНИЕ
Для цифрового шифрования голосовых данных, передаваемых по беспроводному интерфейсу, используется 64-разрядный криптографический ключ. На стороне приема для расшифровки данных используется ключ, вычисляемый на этапе аутентификации.

ДИНАМИЧЕСКАЯ ПЕРЕСТРОЙКА КАНАЛОВ
В рамках реализации протокола DECT устройства динамически перестраиваются на другие каналы при возникновении помех. Непредсказуемость времени перестройки и частоты, на которую перейдет гарнитура, позволяет дополнительно повысить безопасность передачи.

ДИНАМИЧЕСКОЕ РЕГУЛИРОВАНИЕ МОЩНОСТИ
В устройствах DECT компании Plantronics из линейки Savi® и серии CS500 используется функция адаптивного регулирования мощности, в нормальных условиях обеспечивающая снижение уровня мощности радиосигнала, требуемого для осуществления связи, когда пользователь находится рядом с базовой станцией. Для несанкционированного прослушивания переговоров потенциальные инициаторы кибератаки должны находиться в пределах соответствующей зоны действия, либо использовать направленные антенны с высоким коэффициентом усиления, что ограничивает их возможности.

СООТВЕТСТВИЕ ЗАКОНУ САРБЕЙНЗА-ОКСЛИ
Устройства DECT компании Plantronics соответствуют требованиям Статьи 404 Закона Сарбейнза-Оксли (2002 г.). В основе данного заявления лежит соответствие механизмов шифрования, встраиваемых в продукты, требованиям Свода федеральных нормативных актов США (45 CFR 164.312(a)(2)(iv)).

8. Процедура смены ключа во время вызова с использованием нового производного криптографического ключа: криптографический ключ, используемый механизмом шифрования, обновляется не реже одного раза за 60 секунд. Это позволяет предотвратить попытки раскрытия шифра методом перебора, например, с помощью суперкомпьютерных вычислений.

ПРОСТОТА РАЗВЕРТЫВАНИЯ И УПРАВЛЕНИЯ НА ПРЕДПРИЯТИЯХ

В дополнение к гарнитурам серий Savi 400 и Savi 700, поддерживающим новейшие функции DECT, мы предлагаем модернизацию функций DECT на существующих гарнитурах Plantronics с помощью обновления встроенного программного обеспечения. Для этого ИТ-компании могут воспользоваться Plantronics Manager Pro, облачным приложением, предоставляющим уникальные инструменты для управления аудиоустройствами, мониторинга, контроля за соблюдением политик и поддержки пользователей.

Приложение Plantronics Manager Pro входит в пакет программных решений Plantronics Spokes. Оно предлагает ИТ-специалистам простые в использовании инструменты для конфигурирования настроек и обновления микропрограммного и программного обеспечения аудиоустройств для конечных пользователей на предприятии. В состав приложения Plantronics Manager Pro входят средства обработки отчетов, позволяющие ИТ-специалистам составить более полное представление об используемом оборудовании DECT и обеспечить соответствие гарнитур требованиям.

Основные характеристики:

- Включение или выключение функций устройств в соответствии с политикой предприятия или нормативными требованиями
- Предоставление отдельным пользователям возможности обновления настроек DECT в удобное для них время и повышение контроля за их действиями
- Мониторинг настроек и использования аудиоустройства в режиме, близком к реальному времени
- Составления отчетов об инвентаризации и использовании устройств для более рационального использования активов
- Просмотр инвентаризационной информации по всем устройствам, включая устройства других производителе

Компания Plantronics является единственным поставщиком, предлагающим программное обеспечение, которое позволяет ускорить развертывание технологии DECT, поддерживая высокую производительность пользователей и обеспечивая требуемую конфигурацию гарнитур. Благодаря этому, а также устройствам, которые, в отличие от устройств других поставщиков в отрасли, предлагают реальную поддержку расширенных функций DECT, компания Plantronics занимает лидирующие позиции в сфере безопасной беспроводной связи.

Дополнительные сведения см. на веб-сайте plantronics.ru.

[1] Предусмотрена возможность модернизации предыдущих моделей гарнитур Savi 400 и Savi 700 для поддержки новейших функций обеспечения безопасности DECT посредством обновления встроенного ПО.

Не поддерживается для гарнитур серии CS500.