Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Ястребинский
Павел Дмитриевич

Стохастические системы кодирования в радиосистемах передачи данных

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии
по специальности 1-39 81 03 – Информационные радиотехнологии

_____

Научный руководитель
Давыденко Игорь Николаевич
к.т.н., доцент кафедры ИРТ БГУИР

_____

Минск 2018

ВВЕДЕНИЕ

Технология Bluetooth прочно укоренилась в жизни как простого обывателя, пользующегося мобильными устройствами, так и в производстве. беспроводных персональных сетей (Wireless personal area network, WPAN). Bluetooth обеспечивает обмен информацией между такими устройствами, как персональные компьютеры (настольные, карманные, ноутбуки), мобильные телефоны, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики, наушники, гарнитуры на надёжной, бесплатной, повсеместно доступной радиочастоте для ближней связи. Bluetooth позволяет этим устройствам сообщаться, когда они находятся в радиусе до 10 м друг от друга (дальность сильно зависит от преград и помех), даже в разных помещениях.

Работы по созданию Bluetooth начал производитель телекоммуникационного оборудования Ericsson в 1994 году как беспроводную альтернативу кабелям RS-232. Первоначально эта технология была приспособлена под потребности системы FLYWAY в функциональном интерфейсе между путешественниками и системой.

Спецификация Bluetooth была разработана группой Bluetooth Special Interest Group (Bluetooth SIG), которая была основана в 1998 году. В неё вошли компании Ericsson, IBM, Intel, Toshiba и Nokia. Впоследствии Bluetooth SIG и IEEE достигли соглашения, на основе которого спецификация Bluetooth стала частью стандарта IEEE 802.15.1

Принцип действия основан на использовании радиоволн. Радиосвязь Bluetooth осуществляется в ISM-диапазоне (англ. *Industry, Science and Medicine*), который используется в различных бытовых приборах и беспроводных сетях (свободный от лицензирования диапазон 2,4-2,4835 ГГц). В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты (англ. *Frequency Hopping Spread Spectrum, FHSS*). Метод FHSS прост в реализации, обеспечивает устойчивость к широкополосным помехам, а оборудование недорогое.

Согласно алгоритму FHSS, в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду (всего выделяется 79 рабочих частот шириной в 1 МГц, а в Японии, Франции и Испании полоса уже — 23 частотных канала). Последовательность переключения между частотами для каждого соединения является псевдослучайной и известна только передатчику

и приёмнику, которые каждые 625 микросекунд (один временной слот) синхронно перестраиваются с одной несущей частоты на другую. Таким образом, если рядом работают несколько пар приёмник-передатчик, то они не мешают друг другу. Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения. При передаче цифровых данных и аудиосигнала (64 кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно.

Протокол Bluetooth поддерживает не только соединение «point-to-point», но и соединение «point-to-multipoint»

В июне 2006 года была опубликовано подробное описание атаки на устройства Bluetooth. Материал содержал описание как активной, так и пассивной атаки, позволяющей заполучить PIN-код устройства и в дальнейшем осуществить соединение с данным устройством. Пассивная атака позволяет соответствующе экипированному злоумышленнику «подслушать» (sniffing) процесс инициализации соединения и в дальнейшем использовать полученные в результате прослушки и анализа данные для установления соединения (spoofing). Естественно, для проведения данной атаки злоумышленнику нужно находиться в непосредственной близости и непосредственно в момент установления связи. Это не всегда возможно. Поэтому родилась идея активной атаки. Была обнаружена возможность отправки особого сообщения в определённый момент, позволяющего начать процесс инициализации с устройством злоумышленника. Обе процедуры взлома достаточно сложны и включают несколько этапов, основной из которых — сбор пакетов данных и их анализ. Сами атаки основаны на уязвимостях в механизме аутентификации и создания ключа-шифра между двумя устройствами.

На данный момент специальная рабочая группа Bluetooth SIG разрабатывает новые профили, а также новые возможности для изделий, которые используют беспроводную технологию Bluetooth. Данные радио модули раскрывают возможности IoT (Internet of things), развивающегося очень быстрыми темпами и являющейся наиболее перспективной отраслью на рынке мобильных устройств как для обычного потребителя, так и для

индустриальных решений, посему исследования и разработки в данном направлении являются перспективными.

Ввиду повсеместного использования данной технологии в мобильных устройствах, ставших, де-факто, основным способом обмена информации в XXI веке, необходимо задуматься и об обеспечении безопасности и сохранности передаваемой приватной информации на всех уровнях, и в особенности, в наиболее уязвимой на текущий момент связке мобильный телефон – hands free. Таким образом, задача по разработке защищенных систем передачи аудиосигналов является достаточно актуальной

Важным требованием к любой разработке является максимальная доля теоретических исследований. Это позволяет существенно минимизировать затраты труда и материалов на опытное производство и экспериментальные исследования. В данной работе будут рассмотрены ключевые особенности передачи данных по Bluetooth радиоканалу, изучена соответствующая литература, проведено исследование на предмет возможности использования пользовательских алгоритмов шифрования, а также сравнение пользовательских алгоритмов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью настоящей диссертационной работы является исследование механизма шифрования Bluetooth на предмет уязвимостей и реализация пользовательского алгоритма шифрования, в целях повышения крипто устойчивости беспроводного соединения для гарнитуры.

Предмет исследования — методы и способы повышения крипто устойчивости беспроводного Bluetooth соединения. Задачи исследования были поставлены следующие:

1. Изучить техническую документацию и спецификацию Bluetooth, в частности, механизмы установки соединения и авторизации устройств, а так же механизм передачи аудиосигналов по Bluetooth радиоканалу для передачи аудиосигнала на беспроводную гарнитуру.
2. Исследовать стандартный механизм шифрования данных.
3. Исследовать механизм аутентификации Bluetooth соединения на предмет возможности реализации пользовательского механизма шифрования

4. Реализовать на практике и провести сравнительное тестирование пользовательских алгоритмов шифрования RSA и ECC.

Положения, выносимые на защиту

1. Повышение помехозащищенности.
2. Аутентификация устройств и передача аудиосигнала.
3. Повышение защищенности данных путем внедрения алгоритмов шифрования в механизм аутентификации.

Личный вклад магистранта

Все основные выводы по диссертации получены автором лично при непосредственном участии научного руководителя в части осуществления выбора направления исследований и анализа полученных результатов

Опубликованность результатов диссертации

По материалам диссертации опубликована 1 печатная работа, 1 работа — в сборниках статей по материалам конференций.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, пяти глав с выводами, заключения, библиографического списка, 6 приложений с исходным кодом алгоритмов.

Общий объем диссертационной работы составляет 74 страниц, из них 58 страниц основного текста, библиографический список из 20 наименований на двух страницах, и 6 приложений с исходным кодом на 14 страницах.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассматривается актуальность Bluetooth технологии, вводится понятие спецификации Bluetooth, исследуется принцип действия, а так же рассматривается случай атаки на Bluetooth устройства, поднимающий вопрос сохранения пользовательской информации в тайне. Вводится понятие Bluetooth профилей и производится постановка задачи.

В главе один рассматриваются механизмы улучшения производительности в условиях помех (AFH, модифицированный алгоритм AFH компании Erricsson, модификация протокола Link Manager и изменения в интерфейсе хост-контроллера) а также оценивается влияние на вероятность прослушивания.

В главе два рассматриваются базовые профили Bluetooth которые отвечают за общие сообщения и процедуры, используемые для выполнения устройством аутентификации и определения типа устройства.

В главе три рассматриваются профили, имеющие общие модели использования и включающие в себя сообщения и процедуры, используемые для выполнения специфичных команд, в том числе и профили аудиоустройств.

В главе четыре рассматриваются кодеки для кодирования аудиосигнала, производится сравнение частотных характеристик аудиосигналов и делаются выводы относительно использования тех или иных кодеков для передачи человеческой речи.

В главе пять рассматриваются принципы работы защитных механизмов Bluetooth, исследуется стандартная система шифрования и определяются возможные уязвимости. Затем вводится понятие пользовательских алгоритмов шифрования, рассматривается два (один – наиболее распространенный, RSA, а второй – наиболее перспективный ECC) алгоритма шифрования, а так же производится реализация алгоритмов и их сравнительное тестирование. По результатам тестирования делаются выводы относительно целесообразности разработки пользовательских механизмов шифрования.

ВЫВОДЫ

Результаты исследования довольно очевидны: алгоритм ECC превосходит алгоритм RSA и позволяет получать тот же уровень защиты, что и в RSA, но с ключом меньшего размера. Однако, как было сказано выше, существуют классы эллиптических кривых, которые являются слабыми, поэтому для решения проблемы получения надёжных кривых от сомнительных источников следует добавлять случайное порождающее значение (seed) к параметрам области определения. Если посмотреть на стандартизированные кривые NIST, можно увидеть, что они проверяемо случайны.

Если изучить информацию о принципе "в рукавах ничего нет", можно заметить, что:

- Случайные числа для MD5 получаются из синуса целых чисел.
- Случайные числа для Blowfish получаются из первых чисел π.
- Случайные числа для RC5 получаются из e и золотого сечения.

Эти числа случайны, потому что их цифры распределены равномерно. И они не вызывают подозрений, потому что имеют обоснование.

Соответственно, может возникнуть следующий вопрос: откуда берутся случайные порождающие значения для кривых NIST? Ответ: к сожалению, мы не знаем. Эти значения не имеют никакого обоснования.

Возможно ли, что NIST обнаружил некий класс слабых эллиптических кривых, попробовал различные возможные варианты порождающих значений и нашёл уязвимую кривую? На этот вопрос нет ответа, но это закономерный и важный вопрос. Мы знаем, что NIST как минимум успешно стандартизировал уязвимый генератор случайных чисел (генератор, который, как ни странно, основан на эллиптических кривых). Возможно, он успешно стандартизировал и множество слабых эллиптических кривых, однако это, к сожалению, никак не проверить.

Важно понимать, что «проверяемо случайный» и «защищённый» не являются синонимами. И неважно, насколько сложна задача логарифмирования или насколько длинны ключи — если алгоритмы взломаны, то мы ничего не можем поделать.

В этом отношении RSA побеждает, потому что ей не требуются специальные параметры области определения, которые можно эксплуатировать. RSA может быть хорошей альтернативой, если мы не можем доверять властям и если мы не можем создать собственные параметры области определения.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1] Ястребинский П.Д. Использование Bluetooth профилей для передачи аудиосигнала / Ястребинский П.Д. Давыденко. И.Н. // 53-я научная конференция аспирантов магистрантов и студентов БГУИР.