МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
«15» 12 2017 г.

Маскировка телефонного сигнала методом статической перестановки его временных сегментов

Методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22 (076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент
Кандидат технических наук, доцент кафедры информационной безопасности *А.Г. Спеваков*

Маскировка телефонного сигнала методом статической перестановки его временных сегментов: методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко. Курск, 2017. 12 с. Библиогр.: с. 12.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. 15.12.17. Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ 2966. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Цель практической работы

Ознакомление с одним из методов маскировки телефонного сигнала путем перестановки его временных сегментов.

Перед выполнением практического задания студенты должны ориентироваться в основных аспектах информатики, а также иметь начальные знания по программе **Adobe Audition**.

В результате выполнения практического задания студенты должны получить знания по практическому использованию **маскировки телефонного сигнала методом статической перестановки его временных сегментов** на основе использования специальных программных средств.

2 Задание

1. При подготовке к практическому занятию изучить следующие вопросы: методы сигнализации в телефонных сетях, методы генерации сигналов тонального набора номера (DTMF-signals) и шума, методы их редактирования путем разбиения на временные фрагменты и перестановки этих фрагментов в программе Adobe Audition.
2. Запустить программу Adobe Audition, кликнув ее значок на Рабочем столе (если он имеется), либо запустив ее из меню Пуск или с помощью Проводника.
3. Сгенерировать тональный набор произвольного шеститизначного телефонного номера и записать его в тетрадь (сделать скриншот во временной и частотных областях).
4. Пронумеровать временные фрагменты тональных сигналов цифр заданного телефонного номера.
5. Разработать схему скремблирования (т.е. перестановок временных фрагментов тональных сигналов цифр заданного телефонного номера).
6. В соответствии с разработанной схемой перестановок цифр номера, используя компьютерную мышь «вырезать» в буферную память фрагмент тонального сигнала какой-либо выбранной цифры этого номера и вставить ее в заданную схемой перестановок временную позицию.
7. Передать скремблированный сигнал вместе со схемой скремблирования другой подгруппе для дескремблирования.

8. Получить скремблированный сигнал вместе со схемой скремблирования от другой подгруппы для дескремблирования.

9. Дескремблировать сигнал и определить истинный телефонный номер используя опцию Analyze > Show Frequency Analyzis (Показать результат частотного анализа) программы Adobe Audition и Приложение 1.

3 Порядок выполнения работы

1. Изучить методические указания к данному практическому занятию.
2. Получить у преподавателя соответствующий абонентский номер.
3. Выполнить практическую часть
4. Ответить на контрольные вопросы.

4 Содержание отчета

1. Краткие теоретические сведения по методам передачи номера абонента в абонентской линии.
2. Выполненное задание по заданному преподавателем варианту.
3. Временные и спектральные диаграммы (скриншоты) полученных результатов.

5 Теоретическая часть

Основные угрозы конфиденциальности

Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальной информации можно отнести, например, личные данные, учетные записи (имена и пароли), данные о кредитных картах и т.п. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам телекоммуникационной системы (ТКС) (пользователям, процессам, программам). Для остальных субъектов ТКС эта информация должна быть неизвестной.

Защита конфиденциальности – это защита от несанкционированного доступа к информации. Конфиденциальную информацию можно разделить на ***предметную*** и ***служебную***.

Предметная информация относится к определенной ***предметной*** (тематической) области.

Служебная информация (например, пароли пользователей) не относится к определенной ***предметной области***, в инфокоммуникационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной. Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (инфокоммуникационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе. Невозможно помнить много разных паролей; рекомендации по их регулярной смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым и угадываемым паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. В этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т. п).

Основные угрозы конфиденциальности можно разделить на ***технические*** и ***нетехнические***.

К техническим угрозам относят ***перехват*** информации в процессе ее передачи и ***кражу оборудования***, содержащего информацию.

Перехват данных – процесс съема информации, при ее передаче по каналам связи. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их не составляет труда. ***Перехват*** - очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных.

Среди ***нетехнических угроз*** конфиденциальности наиболее опасными являются две угрозы: 1) ***маскарад*** и 2) ***злоупотребление полномочиями.***

Маскарад - выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

Злоупотребление полномочиями - осуществление неправомерных действий, сотрудником, обладающим привилегированными полномочиями.

На многих типах систем привилегированный пользователь (системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример - нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Злоупотребление полномочиями относится к угрозам, от которых трудно защититься.

Конфиденциальность – самый проработанный у нас в стране аспект инфокоммуникационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных ТКС наталкивается на серьезные трудности, зачастую связанные с человеческим фактором.

Методы защиты информации в телефонном канале связи

Методы защиты информации в канале связи можно разделить на две группы:

методы, основанные на ограничении физического доступа к линии и аппаратуре связи и ***методы, основанные на преобразовании***

сигналов в линии к форме, исключающей (затрудняющей) для злоумышленника восприятие или искажение содержания передачи.

Методы первой группы в рассматриваемом варианте построения защищенной связи имеют весьма ограниченное применение, так как на основном протяжении линия связи находится вне ведения субъекта, организующего защиту. В то же время, по отношению к аппаратуре терминала и отдельных участков абонентской линии применение соответствующих мер ограничения физического доступа необходимо.

Ограничение физического доступа предполагает исключение (затруднение):

• непосредственного подключения аппаратуры злоумышленника к электрическим цепям аппаратуры абонентского терминала;

• использования для перехвата информации электромагнитных полей в окружающем пространстве и наводок в отходящих цепях, сети питания и заземления;

• получение злоумышленником вспомогательной информации об используемом оборудовании и организации связи, облегчающей последующее несанкционированное вмешательство в канал связи. При этом должно учитываться не только непосредственное размещение злоумышленника в возможных точках перехвата, но и применение ретрансляторов (―закладок‖, ―жучков‖), визуальная разведка рабочего процесса связи, выявление наличия и характеристик защищенных каналов связи по ПЭМИ.

Применение мер ограничения физического доступа, как правило, нереально для абонента, работающего в *блуждающем* режиме (режиме перемещения в пространстве), но и в этом случае могут быть предприняты отдельные действия.

Методы второй группы направлены на обратимое изменение формы представления передаваемой информации. Преобразование должно придавать информации вид, исключающий ее восприятие при использовании аппаратуры, стандартной для данного канала связи. При использовании же специальной аппаратуры восстановление исходного вида информации должно требовать затрат времени и средств, которые по оценке владельца защищаемой информации делают бессмысленным для злоумышленника вмешательство в информационный процесс.

При защите речевого обмена решающее значение имеет форма представления аналогового речевого сигнала в канале связи. Основные

используемые в настоящее время методы преобразования речевого сигнала и их взаимосвязь показана на рисунке.

Применение вариантов преобразований Б, В и, в большинстве случаев, А требует наличия соответствующей аппаратуры у каждого из взаимодействующих абонентов сети.

При применении наложения защитного шума (вариант А) следует учитывать ряд особенностей:

1. Стойкий защитный эффект оказывает лишь наложение шума, действительно являющегося случайным процессом и по диапазону частот полностью перекрывающего речевой сигнал. В то же время, многие известные и широко применяемые способы получения т. н. ***шумового*** сигнала на самом деле формируют ***псевдошумовой*** сигнал, по ряду своих частотных и временных параметров весьма близкий к действительно шумовому, но на самом деле в значительной степени детерминированный или имеющий существенные внутренние корреляционные связи.

Такой сигнал во многих случаях может полностью заменять шумовой (при измерениях частотных характеристик, оценке помехозащищенности и пр.). Фактическая детерминированность сигнала, как правило, оказывается даже полезной, поскольку облегчает его параметризацию и стабилизацию. Псевдошумовой сигнал, имеющий существенные внутренние корреляционные связи, может быть успешно использован и в качестве защитного шума, если перехват ведется на слух, без использования корреляционной обработки принимаемой или предварительно записанной смеси ***речевой сигнал + шум***.

2. Речевой обмен в естественных условиях подвержен влиянию множества разнообразнейших помех, и в процессе эволюции речевой и слуховой аппарат человека сформировали прекрасно сопряженную и исключительно помехоустойчивую систему. Поэтому, если для технических систем отношение шум/сигнал, необходимое для подавления восприятия сигнала, составляет обычно десятки процентов, то для речи подавление смыслового восприятия происходит при отношении шум/сигнал в несколько сотен процентов, а подавление признаков речи (невозможность фиксации факт разговора) достигается при отношении шум/сигнал близком к 10.

В том же случае, когда ―шумовой‖ сигнал содержит значительную детерминированную составляющую, которая может быть отфильтрована при перехвате, требуемое значение уровня ―шума‖ еще

более возрастает. При оценке защитного эффекта шума ―на слух‖ при отсутствии специальных навыков очень легко ошибиться, т. к. при длительном прослушивании шума и, тем более, при многократном прослушивании записи выявляются многие элементы речи, невоспринимаемые при кратковременной (в течение нескольких секунд) оценке.

3. Следует учитывать, что и защищаемый речевой сигнал и защитный шум распространяются в пространстве и обеспечить полную идентичность распределения их в пространстве крайне сложно. Поэтому во многих случаях защитный шум может быть в значительной степени подавлен методами направленного или многоканального приема. Хорошо известный даже по бытовой звукозаписывающей технике факт: микрофон надо направить на источник звука, при произвольном же расположении микрофона будет записан не столько нужный звук, сколько окружающие шумы. Точно так же высокое отношение шум/сигнал при одном варианте съема сигнала еще не гарантирует столь же высокую эффективность защитного шума при другом варианте съема сигнала, используемого злоумышленником, а при использовании нескольких специально выбранных точек съема может быть ослаблен защитный эффект большинства источников защитного шумового поля. При этом, конечно, нельзя не учитывать, что применение многоканального приема требует как высокой квалификации злоумышленника, так и значительной свободы его действий по отношению к перехватываемому каналу связи.

Для того, чтобы исключить возможность применения нападающей стороной методов многоканального приема можно полностью совместить пути распространения защищаемого сигнала и защитного шума, но тогда будет исключено восприятие речи и абонентом, для которого она предназначена. Чтобы выполнить основную задачу — обеспечить связь, можно было бы предложить формирование идентичных шумовых сигналов на передающей и на приемной стороне.

При этом на передающей стороне шум складывался бы с защищаемым сигналом, а на приемной — вычитался из принимаемого суммарного сигнала. Несмотря на кажущуюся простоту такого варианта, он в течение многих десятилетий не находил реального применения в силу сложности и нестабильности передаточной характеристики канала связи и несовершенства аппаратуры записи и воспроизведения. Компенсация защитного шума на приемной стороне оставалась неполной,

причем ―остаток‖ оказывался неприемлемо большим для качественного восприятия речи принимающим абонентом.

Следует отметить, что в настоящее время в связи с развитием методов цифровой записи и воспроизведения звука и методов цифровой фильтрации с применением быстродействующих сигнальных процессоров, позволяющих обеспечить быструю и точную адаптацию к характеристике канала связи, методы защиты, основанные на полном объединении полезного сигнала и защитного шума в канале связи могут получить новую жизнь.

Варианты Б, В, БВ изменяют форму (спектр) сигнала в канале, проводя перемешивание (скремблирование) отдельных временных или спектральных отрезков исходного сигнала (подробнее реализация таких преобразований рассматривается во второй части стати). При этом в линейном сигнале неизбежно сохраняются отдельные обобщенные признаки преобразуемого речевого сигнала, в которых проявляется взаимная связь перемешиваемых отрезков.

Это принципиально исключает высокую стойкость преобразования. По перехвату сигнала в линии связи при использовании достаточно мощного измерительно-вычислительного комплекса исходная речь может быть с приемлемым для смыслового восприятия качеством восстановлена независимо от примененного закона перестановки, управляющего криптоалгоритма, количества ключей и порядка их ввода.

7 Контрольные вопросы

1. Что такое ***конфиденциальность данных?***

2. На сколько видов и каких можно разделить конфиденциальную информацию?
3. На сколько типов и каких можно разделить основные угрозы конфиденциальности информации?
4. На сколько видов можно разделить технические угрозы?
5. Что такое ***перехват*** сообщений?
6. Сколько выделяют нетехнических угроз и каких?
7. Сколько вариантов и каких возможно для сокрытия (маскировки) аналоговых телефонных сигналов?
8. Сколько вариантов и каких возможно для сокрытия (маскировки) цифровых телефонных сигналов?

Библиографический список

1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.

2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.