шума. Результаты эксперимента согласовываются с литературными данными [4]. Прибор может быть использован для разработки генераторов шума, а так же применяться как встроенный в программно-аппаратный комплекс.

Список литературы

1. А.М. Гришин, Методы защиты речевой информации. // Прикладная Дискретная Математика. – М.:2008. - №2 – С. 67-70.
2. Джеффри Тревис. LabVIEW для всех: Пер. с англ. Клушин Н. А. - М.: ДМК Пресс; ПриборКомплект, 2005. 544 с.
3. Хорев А.А., Макаров Ю.К. К оценке эффективности защиты акустической (речевой) информации // Специальная техника. – М.: 2000. – № 5 – С. 46 - 56.
4. Хорев А.А., Макаров Ю.И. Оценка эффективности систем виброакустической маскировки // Вопросы защиты информации. – М.:2001. - №1 – С. 21 – 28.

ПАССИВНОЕ ПРОСЛУШИВАНИЕ И ПЕРЕХВАТ ПАКЕТОВ В БЕСПРОВОДНОЙ WI-FI-СЕТИ

П.С. Ладыгин, АлтГУ, физико-технический факультет, 3к.
Научный руководитель – ***А.В. Мансуров,*** к.т.н., доцент.

В беспроводной сети, построенной по традиционной технологии Wi-Fi, все беспроводные устройства включены в единую среду доступа, образуя один гигантский «хаб» (концентратор) – и любое беспроводное устройство может «видеть» всех беспроводных соседей в сети. При этом приемник, работающий в пассивном режиме (только прослушивание), вообще невозможно определить. Таким образом становится возможен перехват данных посылаемых клиентом на сервер и соответствующий ответ сервера на запрос. Данную особенность беспроводных сетей может использовать злоумышленник, пользуясь своим Wi-Fi – адаптером, который переключается в режим получения всех пакетов (т.н. promiscous-mode), с последующим разбором и анализом полученной информации. [1,2]

Таким образом, технология перехвата трафика подразумевает прослушивание сети, захват, декодирование, исследование и

интерпретацию данных, передающихся по сети. Целью подобных атак является похищение информации, обычно такой, как идентификационные номера пользователей, данные о функционировании сети, номера кредитных карт, файлов и т.д. Подобная «пассивная» атака, при которой атакующие не могут быть замечены в сети, затрудняет ее определение, делает ее достаточно опасной, но в то же время достаточно интересной для выполнения исследования и разработки законченного программного решения для реализации такой атаки.

Исследование включает в себя разработку программного решения, которое осуществляет перехват информации, передающейся по беспроводной сети, и ее последующую обработку. Перехваченная информация должна пройти дешифрацию (если это необходимо), и дальше подвергнута анализу и обработке для получения осмысленного результата в виде служебных сообщений сети, элементов сетевого обмена, а также законченных логических блоков (файлов), которые могут передаваться по беспроводной сети и содержаться в захваченном сетевом трафике.

Начальным этапом создания программного решения является написание функционала для анализа и обработки данных на уровне стека протоколов. В качестве первого шага реализован процесс анализа стека протоколов со 2 по 7 уровни и обработка наиболее популярного протокола HTTP, что позволяет находить и сохранять в виде отдельных файлов передаваемые по сети документы и объекты (изображения, аудио/видео и пр.)

Для захвата пакетов пользователь выбирает сетевую карту, которая переводится в т.н. promiscous-режим. Следует отметить, что не каждая карта имеет такую функциональную возможность. Далее осуществляется захват пакетов.

Стандартной процедурой начала сетевого обмена между компьютером «жертвы» и сервером по протоколу TCP [3] является передача пустого пакета с флагом SYN=1. Зафиксировав этот флаг, рабочая программа создает поток, в который будет помещаться вся информация, посылаемая на сервер. Далее, сервер отвечает своему клиенту на запрос тоже пустым пакетом с флагом SYN=1, что создает второй поток. Туда будет записываться вся информация, отправляемая сервером клиенту. После этого происходит обмен между компьютером «жертвы» и сервером при по-

мощи протокола более высокого уровня (HTTP), который сохраняется в созданные потоки.

На рис. 1 изображен пример сохраненного html-запроса.

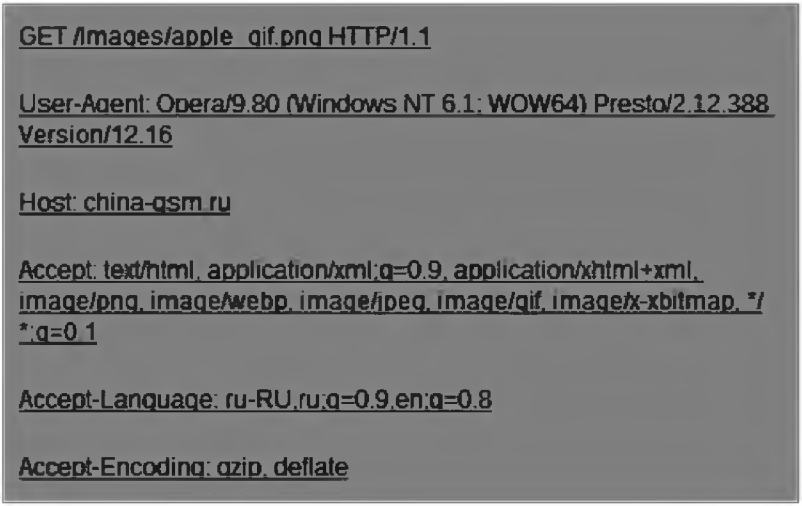

Рис.1. Пример сохраненного html-запроса.

На рис.1 можно увидеть, что компьютер «жертвы» запрашивает изображение с расширением .png, программа фиксирует название этого изображения («apple_gif.png») и запоминает. Помимо этого в запросе может содержаться информация об аутентификации, пароли, сообщения, запрашиваемая информация для поисковых систем и др., которая также сохраняется программой.

Далее, сервер отвечает компьютеру «жертвы» на запрос пакетом, содержащим сообщение с кодом 200 OK [4] (рис.2). Это означает что соответствующий запрос получен. Внутри этого пакета содержится само изображение (на это указывает поле «Content-type»). Рабочая программа фиксирует начало передаваемого изображения и в отдельный поток отправляет код этого изображения. Помимо изображения сервер может отвечать и html-документом, и архивом, и другой информацией, которая также сохраняется программой.

Рис.2. Пример сохраненного html – ответа.

Трудоемким в процессе перехвата пакетов является осуществление дешифрации содержимого кадров сетевого обмена (при использовании алгоритмов шифрования WEP, WPA и др. [5]), а также анализ и работа со стеком используемых в сети протоколов от сетевого до самого высокого прикладного уровня.

Таким образом, рабочая программа представляет с собой приложение, позволяющее осуществлять перехват пакетов, передающихся по беспроводной Wi-Fi — сети. Программа анализирует полученные данные, вплоть до седьмого уровня стека протоколов, сохраняет информацию, передающуюся по протоколу HTTP, в отдельные файлы, согласно её типу. Вся информация, которая передается согласно другим протоколам или зашифрована сохраняется в «сыром» виде, что позволяет производить её анализ отдельно.

Дальнейшая работа планируется над расширением функциональности модуля анализа и обработки стека протоколов, а также поддержку процедур дешифровки захваченного трафика, анализа служебной информации беспроводной сети и сохранение критичного информационного обмена сетевых сервисов, отвечающих за вопросы аутентификации, авторизации и контроля доступа к сетевым ресурсам локальной сети.

Список литературы

1. Олифер В.Г. Компьютерные сети (принципы, технологии, протоколы) 3-е издание / В.Г. Олифер, Н.А. Олифер - СПб.:«Питер», 2006. - 284 с.

2. Безопасность сетей 802.11 — основные угрозы/Хабрахабр. [Электронный ресурс]. // Режим доступа: http://habrahabr.ru/post/151126/. - Загл. с экрана. Дата обращения: 31.04.2014.
3. Танненбаум Э. Компьютерные сети. 4-е изд. / Э. Танненбаум - СПб.: «Питер», 2003. - 572 с.
4. Танненбаум Э. Компьютерные сети. 4-е изд. / Э. Танненбаум - СПб.: «Питер», 2003. - 736 с.
5. Мэрритт М. Безопасность беспроводных сетей / М. Мэрритт, Д. Поллино; Пер. с англ. А.В. Семенова — М.: Компания АйТи; ДМК Пресс, 2004. - 288 с.

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ОЦЕНКИ ЗАЩИЩЕННОСТИ АКУСТИЧЕСКОГО КАНАЛА СВЯЗИ

А.В. Одинцова, АлтГУ физико-технический факультет, 5 к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

В настоящее время существуют несколько методик оценки разборчивости речи в акустическом канале связи. Применительно к оценке защищенности речевой информации наибольшую популярность получили формантные методы, которые, в сущности, являются различными версиями единого формантного подхода.

Многообразие версий объясняется недостаточной изученностью вопросов формантой разборчивости речи. Для проведения исследований в этой области необходима гибкая система по оценке защищенности акустического канала связи, позволяющая использовать и сравнивать различные методы. Представленные на рынке аппаратно-программные комплексы используют закрытые алгоритмы вычисления разборчивости речи, что является неприемлемым для научных исследований.

В настоящей работе разработана автоматизированная система оценки защищенности акустического канала связи, которая позволяет оценивать уровень разборчивости речи, используя различные методики.

Ключевым понятием в теории разборчивости речи является понятие форманта, которая характеризует области максимальной