Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Кузбасский государственный технический университет
имени Т. Ф. Горбачева»

С. А. Асанов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Рекомендовано учебно-методической комиссией специальности
230201 «Информационные системы и технологии» в качестве
электронного издания для использования в учебном процессе

Кемерово 2012

Рецензенты:

Г.А. Алексеева – старший преподаватель кафедры ИиАПС

В.А. Полетаев – проф., д.т.н., председатель УМК специальности 230201 «Информационные системы и технологии»

Асанов Сергей Александрович. Информационная безопасность и защита информации: методические указания к лабораторным работам [Электронный ресурс] для студентов очной формы обучения специальности 230201 «Информационные системы и технологии» / С. А. Асанов. Электрон. дан. – Кемерово: КузГТУ, 2012. – 1 электрон. опт. диск (CD-ROM); зв.; цв.; 12 см. – Систем. требования: Pentium II; ОЗУ 8 Мб; Windows 95; (CD-ROM-дисковод); мышь. – Загл. с экрана.

В данных методических указаниях изложены содержания лабораторных работ, порядок их выполнения и контрольные вопросы к ним.

ЛАБОРАТОРНАЯ РАБОТА № 1. КОМПЬЮТЕРНЫЕ ВИРУСЫ

1.1. ЦЕЛЬ РАБОТЫ

Целью данной лабораторной работы является ознакомление студентов с основными видами вредоносного программного обеспечения и методами борьбы с ним.

1.2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

1.2.1. Основные положения

Компьютерным вирусом называется программа (некоторая совокупность выполняемого кода/инструкций), которая способна создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты/ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Вирусы можно разделить на классы по следующим признакам:

а) по среде обитания вируса;

б) по способу заражения среды обитания;

в) по деструктивным возможностям;

г) по особенностям алгоритма вируса.

По среде обитания вирусы можно разделить на сетевые, файловые и загрузочные. Сетевые вирусы распространяются по компьютерной сети, файловые внедряются в выполняемые файлы, загрузочные – в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Существуют сочетания – например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы и часто применяют оригинальные методы проникновения в систему.

Способы заражения делятся на резидентный и нерезидентный. Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая за-

тем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

По деструктивным возможностям вирусы можно разделить на:

1) безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

2) неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;

3) опасные вирусы, которые могут привести к серьезным сбоям в работе;

4) очень опасные, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

По особенностям алгоритма можно выделить следующие группы вирусов:

Компаньон-вирусы (companion) – это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл.

Вирусы-«черви» (worm) – вирусы, которые распространяются в компьютерной сети и, так же как и компаньон-вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы,

но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

«Паразитические» – все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются «червями» или «компаньон».

«Стелс»-вирусы (вирусы-невидимки, stealth), представляющие собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

«Полиморфик»-вирусы (самошифрующиеся или вирусы-призраки, polymorphic) – достаточно труднообнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

«Макро-вирусы» – вирусы этого семейства используют возможности макро-языков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время наиболее распространены макро-вирусы заражающие текстовые документы редактора Microsoft Word.

1.2.2. Симптомы вирусного поражения компьютера

Основные симптомы вирусного поражения следующие:

- Замедление работы некоторых программ.
- Увеличение размеров файлов (особенно выполняемых).
- Появление не существовавших ранее «странных» файлов.
- Уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы).
- Внезапно возникающие разнообразные видео и звуковые эффекты.

При всех перечисленных выше симптомах, а также при других «странных» проявлениях в работе системы (неустойчивая работа, частые «самостоятельные» перезагрузки и прочее) настоятельно рекомендуется, немедленно произвести проверку на наличие вирусов с помощью антивирусных продуктов последних версий и с самыми свежими обновлениями антивирусных баз.

1.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Поместить на внешний носитель тестовый файл EICAR.
2. Установить в лабораторной среде антивирусное программное обеспечение, соответствующее индивидуальному заданию.
3. Деактивировать резидентную защиту антивирусного программного обеспечения, скопировать с внешнего носителя тестовый файл EICAR на рабочий стол лабораторной системы.
4. Активировать резидентную защиту антивирусного программного обеспечения. Убедиться, что тестовый файл обнаружен средствами резидентной защиты и удален.
5. С помощью средств антивирусного программного обеспечения произвести проверку внешнего носителя, содержащего тестовый файл EICAR. Убедиться, что тестовый файл обнаружен и удален.
6. В соответствии с индивидуальным заданием изучить работу антивирусного программного обеспечения при попытке внедрить тестовый файл EICAR в лабораторную систему по различным каналам распространения вирусов.

1.4. ОБРАЗЕЦ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ

ОС лабораторной среды: Windows XP SP2.
Антивирусное ПО: Dr.Web Security Space.
Дополнительный канал проникновения: e-mail.

1.5. ФОРМА ОТЧЕТНОСТИ

Журнал работы антивирусного программного обеспечения с выделенными событиями обнаружения и удаления тестового файла должен быть назван по формату **ФамилияИмяОтчество_НомерГруппы_ДатаВыполненияРаботы** и помещён в папку, указанную преподавателем.

1.6. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое компьютерный вирус?
2. Классификация компьютерных вирусов.
3. Что такое троянские программы и другое вредоносное программное обеспечение, не являющееся вирусами?
4. Способы заражения исполняемых программ.
5. Что такое загрузочные вирусы?
6. Что такое резидентные вирусы?
7. Что такое полиморфные вирусы?
8. Основные каналы проникновения вирусов в систему.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. http://ru.wikipedia.org/wiki/Eicar
2. http://ru.wikipedia.org/wiki/Антивирусная_программа
3. http://ru.wikipedia.org/wiki/Компьютерный_вирус
4. Михайлов А. В. Компьютерные вирусы и борьба с ними. – М.: Диалог МИФИ, 2010. – 104 с.

ЛАБОРАТОРНАЯ РАБОТА № 2. ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ СПЕЦИАЛИЗИРОВАННЫХ УТИЛИТ ШИФРОВАНИЯ И СЖАТИЯ ДАННЫХ

2.1. ЦЕЛЬ РАБОТЫ

Целью работы является ознакомление студентов с принципами совместного использования шифрования, помехоустойчивого кодирования и сжатия информации для комплексной защиты информации в процессе ее передачи и хранения.

2.2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

2.2.1. Проблемы передачи информации и их комплексное решение

В процессе передачи информации от источника к потребителю на информацию воздействуют различные неблагоприятные факторы. Криптографические методы защищают информацию только от одного вида разрушающих воздействий – от предумышленного разрушения или искажения информации. Однако на практике, при передаче информации от абонента к абоненту, возможны случайные помехи на линиях связи, ошибки и сбои аппаратуры, частичное разрушение носителей данных и т.д. Таким образом, в реальных системах связи существует проблема защиты информации от случайных воздействий.

В связи с появлением сетей передачи данных высокой пропускной способности и развитием мультимедиа-технологий возникает проблема шифрования больших объемов информации. Если раньше основным типом шифруемых и передаваемых сообщений было текстовое сообщение, то в XXI веке криптографическая защита все чаще применяется при передаче цифровых видео- и речевых сообщений, карт местности, для организации видеоконференций. Именно поэтому в последнее время возникает проблема шифрования огромных информационных массивов. Для интерактивных систем типа телеконференций, организации аудио- или видеосвязи, такое шифрование должно осуществлять-

ся в реальном режиме времени и по возможности быть незаметным для пользователей.

Решение указанных проблем, в том числе и защита от несанкционированного доступа, может быть достигнуто при комплексном использовании достижений теории информации.

В теории информации выделяют три вида преобразования информации: криптографическое шифрование, помехоустойчивое кодирование и сжатие (или компрессия). В некоторых научных работах XX века все три вида преобразования информации называли кодированием: криптографическое кодирование, помехоустойчивое кодирование и эффективное кодирование (сжатие данных). Общим для всех трех видов преобразования является то, что информация каким-либо образом меняет форму представления, но не смысл. Отличия разных видов кодирования связаны с целью проводимых преобразований.

Так, целью криптографического преобразования является, как известно, защита от несанкционированного доступа, аутентификация и защита от преднамеренных изменений. Помехоустойчивое кодирование выполняется с целью защиты информации от случайных помех при передаче и хранении. Эффективное кодирование производится с целью минимизации объема передаваемых или хранимых данных.

На практике эти три вида преобразования информации обычно используются совместно. Так, например, некоторые программные пакеты перед шифрованием архивируют обрабатываемые данные. С другой стороны, реальные системы передачи информации, будь то локальные и глобальные сети передачи данных, или компьютерные носители информации (CD или DVD-диски) всегда имеют в составе системы защиты информации средства контроля и коррекции случайных ошибок.

Таким образом, криптографическое шифрование, помехоустойчивое кодирование и сжатие отчасти дополняют друг друга и их комплексное использование помогает эффективно использовать каналы связи для надежной защиты передаваемой информации.

Для того, чтобы более эффективно использовать на практике криптографические методы защиты информации, рассмотрим

основные положения теорий помехоустойчивого и эффективного кодирования, используемые в системах защиты информации.

2.2.2. Помехоустойчивое кодирование

Как уже отмечалось, вопросы криптографического преобразования информации тесно связаны с вопросами помехоустойчивого кодирования сообщений. Это обусловлено, с одной стороны (теоретической), тем, что и при криптографическом шифровании, и при помехоустойчивом кодировании используются одни и те же законы теории информации. С другой стороны (практической) процессы накопления, хранения и передачи информации протекают в условиях воздействия помех, способных исказить хранимые и обрабатываемые данные. Это обуславливает актуальность разработки и использования методов, позволяющих обнаруживать и корректировать подобные ошибки. С математической точки зрения задача сводится к синтезу так называемых **помехоустойчивых кодов**.

Аналогично понятию шифра в криптографии при обсуждении помехоустойчивого кодирования и вопросов сжатия сообщений вводят понятие кода. Вообще **кодом** называется совокупность знаков, а также система правил, позволяющая представлять информацию в виде набора таких знаков. **Кодовым словом** называют любой ряд допустимых знаков. Например, двоичное число 1100 можно считать двоичным 4-разрядным кодовым словом.

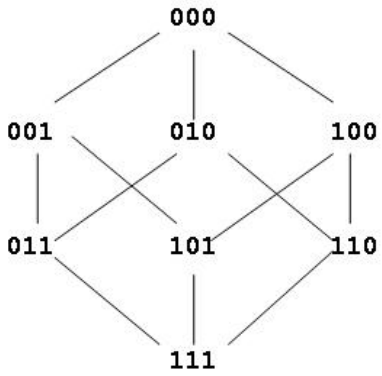
Общая идея помехоустойчивого кодирования состоит в том, что из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые из них. Например, в коде с контролем по четности считаются допустимыми лишь слова с четным числом единиц. Ошибка превращает допустимое слово в недопустимое и поэтому обнаруживается.

Помехоустойчивые коды делятся на блоковые, делящие информацию на фрагменты постоянной длины и обрабатывающие каждый из них в отдельности, и свёрточные, работающие с данными как с непрерывным потоком.

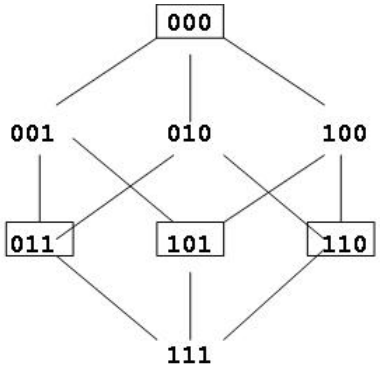
Блоковые коды характеризуются так называемым минимальным кодовым расстоянием. Вообще, **расстоянием по Хэммингу** (по имени американского математика Р.У. Хэмминга) ме-

жду двумя кодовыми словами называется число разрядов, в которых они различны. При этом в качестве **минимального кодового расстояния** выбирается наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код.

Например, пусть мы используем только трехразрядные двоичные слова. Всего таких кодовых слов может быть восемь. Те кодовые слова, которые отличаются только на одну единицу, называются **соседними**. Например, кодовые слова 101 и 111 – соседние, так как отличаются только средним разрядом, а слова 101 и 110 – не соседние, так как у них отличаются два последних разряда. Изобразим все трехразрядные двоичные комбинации и соединим линией соседние кодовые слова. Минимальное кодовое расстояние между словами обычного, не помехоустойчивого кода равно единице.



В случае использования всех трехразрядных двоичных слов для передачи сообщений все они будут считаться допустимыми. Применим контроль по условию четности. Тогда допустимыми будут только выделенные рамками слова с четным числом единиц.



Минимальное расстояние между допустимыми словами кода с контролем по четности равно двум (из рисунка видно, что никакие два кодовых слова в рамках не соединены линиями, то есть не являются соседними). Именно по этой причине одиночная ошибка в кодовом слове превращает это слово в недопустимое.

Платой за помехоустойчивость является необходимость увеличения длины слов по сравнению с обычным кодом. В данном примере только два разряда являются информационными. Это они образуют четыре разных слова. Третий разряд является контрольным и служит только для увеличения расстояния между допустимыми словами. В передаче информации контрольный разряд не участвует, так как является линейно зависимым от информационных. Код с контролем по четности, рассмотренный в качестве примера, позволяет обнаружить одиночные ошибки в блоках данных при передаче данных. Однако он не сможет обнаружить двукратные ошибки потому, что двукратная ошибка переводит кодовое слово через промежуток между допустимыми словами и превращает его в другое допустимое слово.

Таким образом, для того чтобы код приобрел способность к обнаружению и коррекции ошибок, необходимо отказаться от его безызбыточности. Для этого и разделяют всё множество возможных комбинаций двоичных символов на два подмножества: допустимых кодовых слов и недопустимых. Разбиение осуществляется таким образом, чтобы увеличить минимальное кодовое расстояние между допустимыми словами. В этом случае любая однократная ошибка превращает допустимое кодовое слово в недопустимое, что позволяет её обнаружить.

Естественно, что введение дополнительных контрольных разрядов увеличивает затраты на хранение или передачу кодированной информации. При этом фактический объем полезной информации остается неизменным. В этом случае можно говорить об **избыточности** помехоустойчивого кода, которую формально можно определить как отношение числа контрольных разрядов к общему числу разрядов кодового слова.

Мы уже отмечали, что контрольные разряды не передают информацию и в этом смысле бесполезны. Относительное число контрольных разрядов называется избыточностью Q помехоустойчивого кода:

$$Q = k / n \cdot 100\%$$

где k – число контрольных двоичных разрядов; n – общее число двоичных разрядов в блоке.

Например, избыточность рассмотренного трехразрядного кода с контролем по четности составляет:

$$Q = 1 / 3 \cdot 100\% \approx 33{,}33\%$$

Избыточность является важной характеристикой кода, причем чрезмерное увеличение избыточности нежелательно. Важной задачей теории информации является синтез кодов с минимальной избыточностью, обеспечивающих заданную обнаруживающую и корректирующую способность.

2.2.3. Принципы сжатия данных

Как было сказано выше, одной из важных задач предварительной подготовки данных к шифрованию является уменьшение их избыточности и выравнивание статистических закономерностей применяемого языка. Частичное устранение избыточности достигается путём сжатия данных.

Сжатие информации представляет собой процесс преобразования исходного сообщения из одной кодовой системы в другую, в результате которого уменьшается размер сообщения. Алгоритмы, предназначенные для сжатия информации, можно разделить на две большие группы: реализующие сжатие без потерь (обратимое сжатие) и реализующие сжатие с потерями (необратимое сжатие).

Обратимое сжатие подразумевает абсолютно точное восстановление данных после декодирования и может применяться для сжатия любой информации. Оно всегда приводит к снижению объема выходного потока информации без изменения его информативности, то есть без потери информационной структуры. Более того, из выходного потока, при помощи восстанавливающего или декомпрессирующего алгоритма, можно получить входной, а процесс восстановления называется декомпрессией или распаковкой и только после процесса распаковки данные пригодны для обработки в соответствии с их внутренним форматом. Сжатие без потерь применяется для текстов, исполняемых файлов, высококачественного звука и графики.

Необратимое сжатие имеет обычно гораздо более высокую степень сжатия, чем кодирование без потерь, но допускает некоторые отклонения декодированных данных от исходных. На практике существует широкий круг практических задач, в которых соблюдение требования точного восстановления исходной информации после декомпрессии не является обязательным. Это, в частности, относится к сжатию мультимедийной информации: звука, фото- или видеоизображений. Так, например, широко применяются форматы мультимедийной информации JPEG и MPEG, в которых используется необратимое сжатие. Необратимое сжатие обычно не используется совместно с криптографическим шифрованием, так как основным требованием к криптосистеме является идентичность расшифрованных данных исходным. Однако при использовании мультимедиа-технологий данные, представленные в цифровом виде, часто подвергаются необратимой компрессии перед подачей в криптографическую систему для шифрования. После передачи информации потребителю и расшифрования мультимедиа-файлы используются в сжатом виде (то есть не восстанавливаются).

Таким образом, криптографическое шифрование, помехоустойчивое кодирование и сжатие отчасти дополняют друг друга и их комплексное использование помогает эффективно использовать каналы связи для надежной защиты передаваемой информации.

1.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить у преподавателя индивидуальное задание: список алгоритмов кодирования и/или сжатия данных;
2. Изучить принципы работы алгоритмов, указанных в индивидуальном задании;
3. Установить программное обеспечение, реализующее работу указанных алгоритмов;
4. С помощью программного обеспечения выполнить обработку данных (тип данных указан в индивидуальном задании) указанными алгоритмами;
5. С помощью утилит нахождения разности между двумя наборами данных сформировать файл отчёта.

1.4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие виды преобразований информации используются для комплексной защиты информации?
2. Каковы основные принципы помехоустойчивого кодирования сообщений?
3. Как рассчитать избыточность помехоустойчивого кода?
4. Приведите примеры алгоритмов, обеспечивающих сжатие сообщений.
5. Для каких типов данных целесообразно использовать алгоритмы сжатия с потерями? С чем это связано?

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. http://www.intuit.ru/department/security/bcript/
2. http://www.chhm.net/index.php?articles=91
3. http://www.univer.omsk.su/omsk/Edu/infpro/all.html
4. Ватолин Д., Ратушняк А. и др. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: Диалог-МИФИ, 2003. – 384 с.

ЛАБОРАТОРНАЯ РАБОТА № 3. ПАРОЛЬНАЯ ЗАЩИТА ИНФОРМАЦИИ

3.1. ЦЕЛЬ РАБОТЫ

Целью работы является ознакомление студентов с системами защиты информации с использованием паролей, а также, с типовыми угрозами информации, при использовании парольной защиты.

3.2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

3.2.1. Общие сведения

Наиболее распространенной системой защиты информации в настоящее время является использование паролей (ключевых фраз) в том или ином виде. Основной причиной широкого распространения данных методов является простота их реализации.

При рассмотрении систем парольной защиты используются следующие понятия:

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

База данных идентификаторов – хранилище всех идентификаторов системы, используемое в процедуре аутентификации.

3.2.2. Общие подходы к построению парольных систем

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. В первую разновидность способов входят системы аутентифика-

ции, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных идентификаторов, содержащую данные для всех пользователей Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации. Общий подход к применению одноразовых паролей основан на последовательном использовании хеш-функции для вычисления очередного одноразового пароля на основе предыдущего. Вначале пользователь получает упорядоченный список одноразовых паролей, последний из которых также сохраняется в системе аутентификации. При каждой регистрации пользователь вводит очередной пароль, а система вычисляет его свертку и сравнивает с хранимым у себя эталоном. В случае совпадения пользователь успешно проходит аутентификацию, а введенный им пароль сохраняется для использования в качестве эталона при следующей регистрации. Защита от сетевого перехвата в такой схеме основана на свойстве необратимости хеш-функции. Наиболее известные практические реализации схем с одноразовыми паролями – это программный пакет S/KEY и разработанная на его основе система OPIE.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен «троянский конь»). Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена, Корректность протоколов аутентификации вытекает из свойств задейст-

вованных в них математических и криптографических преобразований и может быть строго доказана.

3.2.3. Методы преодоления парольной защиты

Узнавание пароля. Часто пользователи записывают пароли на листках, в блокнотах, тетрадях, доступных неавторизованным лицам. Доступность записанных паролей, их несекретность, является одной из важных «дыр» в парольной защите. Часто пароли доступа могут быть получены путем их выведывания, обычно с использованием тех или иных методов психологии или социальной инженерии. Разновидностью этого метода является выведывание информации, которая могла быть использована пользователем в подсказках, иногда предусматриваемых на случай, если пароль забыт. Такие подсказки предлагаются, например, почтовыми серверами при регистрации электронного почтового ящика и, обычно, представляются предложением ответить на некоторый контрольный вопрос, такой как «Ваш рост», «Ваше любимое блюдо», «номер Вашего паспорта», «девичья фамилия матери» и т. п. Для желающего получить доступ к защищенному паролем ресурсу, как правило, значительно легче узнать информацию, необходимую для правильного ответа на подобные вопросы, чем сам пароль.

Угадывание пароля. Во многих случаях в качестве пароля используются имена, фамилии, номера телефонов и другие личные данные пользователя или его родственников и друзей. Такая информация может быть известна злоумышленникам, что позволяет использовать ее для угадывания и подбора пароля. В наиболее примитивном случае пароль выбирается пользователем таким же как учетное имя (логин).

Словарная атака. Наиболее распространенным вариантом при выборе пароля является задание в качестве пароля некоторого слова, что, в первую очередь, обусловлено легкостью запоминания такого пароля. В этом случае пароль может быть выявлен при помощи специальных программ-взломщиков паролей, реализующих, так называемую, словарную атаку, состоящую в последовательном переборе всех слов, содержащихся в электронном словаре, подключаемом к такой программе. В настоящее время

для определения пароля разработан ряд специальных словарей, опубликованных или размещенных в Интернете. Такие словари содержат сотни тысяч слов, имен, названий, наиболее часто употребляемых в качестве паролей, в том числе географических, названий корпораций, торговых марок, названий кинофильмов, спортивных клубов и т.п. Словарный перебор осуществляется очень быстро, особенно, если словарь составлен как частотный, в котором слова расположены с учетом частоты их использования в качестве паролей.

Метод прямого перебора (brute-force attack – метод грубой силы, «лобовая атака»). Этот метод предполагает прямой перебор всех возможных комбинаций всех допустимых в пароле символов. Перебор символов осуществляется до тех пор, пока не будет найдена нужная комбинация. Описанные выше способы преодоление парольной защиты путем узнавания или угадывания пароля с перебором ограниченного количества сочетаний букв, цифр и символов, вводимых с клавиатуры, может привести к успеху лишь в том случае, когда пользователь игнорирует элементарные правила выбора пароля. Словарная атака эффективна лишь при игнорировании пользователем одного из основных правил выбора пароля – не использовать в качестве пароля семантически определенное слово. Если выбран нетривиальный и достаточно длинный пароль, его успешный подбор возможен только методом прямого перебора.

Использование программных закладок. Для добывания паролей, хранящихся в памяти компьютера, в том числе, системных паролей могут использоваться специальные программы – программные закладки, скрытно устанавливаемые в атакуемый компьютер с целью получения информации о пользовательских паролях. К наиболее распространенной разновидности программных закладок – перехватчиков паролей – относятся программы, которые будучи внедренными в операционную систему, получают доступ к паролям, вводимым пользователями, перехватывают их, записывают в специальный файл или в другое место, доступное злоумышленнику, внедрившему закладку в систему.

Непосредственный доступ к компьютеру. Если возможен непосредственный доступ злоумышленника к защищенному компьютеру, то им может быть получена информация, записанная в

компьютере, включая данные о паролях, включая пользовательские учетные записи и системные пароли. Такие атаки возможны, если в политике безопасности или при администрировании компьютерной системы допущены ошибки, в частности не перекрыта возможность загрузки операционной системы с внешних носителей (дискет, CD, DVD). В этом случае любая информация с атакованного компьютера может быть скопирована и подвергнута анализу. В частности, становится возможным подбор пароля, даже если он хранился в компьютере в зашифрованном виде.

Перехват паролей с использованием технических средств. Использование технических каналов утечки для получения конфиденциальной, в том числе парольной, информации является весьма непростой, но решаемой задачей. В подавляющем большинстве случаев используются электромагнитный и электрический каналы утечки, реже – оптический канал, предполагающий возможность визуального наблюдения за процессом ввода информации. Такое наблюдение может осуществляться с использованием оптических приборов или видеокамер. Крайне опасными следует считать устройства, предназначенные для перехвата сигналов клавиатуры – аппаратно реализованные клавиатурные мониторы. Такое устройство может быть скрытно установлено на провод клавиатуры или как «переходник» между системным блоком и разъемом клавиатуры, либо внутри системного блока. В этом случае вся набираемая на клавиатуре информация перехватывается и передается, как правило, по радиоканалу.

3.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить у преподавателя индивидуальное задание: файл с базой данных идентификаторов и программы для аудита паролей.
2. Изучить принципы работы алгоритмов, указанных в индивидуальном задании.
3. С помощью программного обеспечения выполнить аудит паролей, используя различные виды перебора.
4. Сформировать отчёт, содержащий расшифрованную базу данных идентификаторов.

3.4. ФОРМА ОТЧЕТНОСТИ

Расшифрованную базу данных идентификаторов назвать по формату **ФамилияИмяОтчество_НомерГруппы_ДатаВыполненияРаботы** и поместить в папку, указанную преподавателем.

3.5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Объясните разницу между процессами аутентификации и идентификации.
2. Какие системы аутентификации Вы знаете?
3. Сформулируйте основные требования к созданию стойких паролей.
4. Перечислите преимущества и недостатки систем парольной защиты.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. http://www.gsm-guard.net/press2_4.html
2. http://www.zashita-informacii.ru/node/85
3. http://www.intuit.ru/department/internet/iissecurity/9/9.html

ЛАБОРАТОРНАЯ РАБОТА № 4. ГРАФОВАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ОБЪЕКТОВ ИНФОРМАЦИОННЫХ СЕТЕЙ

4.1. ЦЕЛЬ РАБОТЫ

Целью работы является ознакомление студентов с графовой моделью взаимодействия объектов информационных сетей, как инструмента анализа механизмов реализации типовых угроз безопасности.

4.2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

Графовая модель взаимодействия объектов информационных сетей предназначена для анализа механизмов реализации типовых угроз безопасности в данной информационной сети. На входе у модели находится адрес объекта, с которого передается сообщение и на который необходимо доставить сообщение; на выходе – итоговый результат (доставлено ли сообщение). Основная задача данной модели РВС состоит в формировании на графе пути между заданными входными параметрами модели (между двумя объектами).

Модель в проекции на физический уровень OSI определяет, как физически связаны и сообщаются между собой объекты РВС; в проекции на канальный уровень OSI устанавливает взаимодействие объектов на уровне аппаратных адресов сетевых адаптеров; а в проекции на сетевой уровень OSI определяет связь объектов на уровне логических адресов, например адресов IP.

Пусть имеется распределённая вычислительная сеть, включающая в себя N связанных между собой KS (линиями связи на физическом и канальном уровне) и LS (линиями связи на сетевом уровне OSI) объектов (M хостов x_i и N(M + 1) и роутеров g_i, где i = 1..M и J = M + 1..N; M < N). Так как модель распределённой вычислительной сети в проекции на физический уровень ничем не отличается от той же модели в проекции на канальный уровень, то ограничимся введением **универсальной линии связи KS,** под которой будем понимать линию связи либо физического, либо канального уровня OSI.

На физическом уровне под объектом понимается сетевой адаптер хоста или роутера, на канальном – аппаратный адрес сетевого адаптера. На этих уровнях модели выделим из всего множества хостов $N – (M + 1)$ подмножество X_k, где $k = 1..N – (M + 1)$, по числу роутеров в РВС, каждое из которых связано на физическом и канальном уровнях только с одним ближайшим роутером и представляет собой сетевой сегмент. Соответственно все объекты внутри данного подмножества X_k взаимодействуют между собой при помощи двунаправленных линий связи физического или канального уровня ks_{ij}, соединяющих i-объект с j-объектом; также каждый объект из подмножества X_k связан с соответствующим роутером G_{m+k}, через который и только через который объект из данного множества (сегмента) может сообщаться с объектом из другого множества (сегмента). Это правило будет введено для упрощения модели, так как при моделировании механизмов атак связь объекта сразу с несколькими роутерами не играет роли. Таким образом, на канальном и физическом уровнях модели из вершины X_k попасть в вершину X_{k-p} ($p < k$) можно только в том случае, если они находятся в одном подмножестве или путь проходит через последовательность узлов из множества G, следовательно, путь между любыми двумя объектами из множества X не может проходить через другой, отличный от них транзитный объект из того же множества.

На сетевом уровне под объектом понимается сетевой адрес хоста или роутера. На этом уровне каждый объект может взаимодействовать с любым другим объектом РВС при помощи однонаправленной или двунаправленной линии связи сетевого уровня ls_{ij}, соединяющей i-объект с j-объектом.

Введем два правила. Во-первых, все объекты внутри одного подмножества X_k (сегмента) всегда связаны между собой физически, но не всегда соединены канальными линиями связи, а следовательно, на данном уровне все объекты **потенциально** могут быть связаны друг с другом линией канального уровня, но могут быть и не связаны.

Во-вторых, путь на K-ом уровне модели OSI между двумя объектами РВС существует тогда и только тогда, когда он существует на всех уровнях от 1 до $K – 1$, где $1 < K \leq 7$. Исключением является случай, когда между двумя объектами из одного под-

множества (сегмента) X_k нет пути на канальном уровне, но существует путь на сетевом (широковещательный сетевой запрос (например, ARP), который получат все объекты в данном сегменте).

Согласно предлагаемой модели:

$X = \{x_i \mid i = 1..M\}$ – множество хостов;

$G = \{g_j \mid j = M + 1..N\}$ – множество роутеров;

$KS = \{ks_{kL} \mid k = 1..N,\ L = 1..N\ \}$ – множество линий связи объектов на физическом или канальном уровне OSI; ks_{kL} – линия связи k-го объекта с объектом L;

$LS = \{ls_{kL} \mid k = 1..N,\ L = 1..N\}$ – множество линий связи объектов на сетевом уровне OSI; ls_{kL} – линия связи k-го объекта с объектом L;

$X_k = \{x_p \mid p = 1..M\}$ – подмножество хостов внутри одного сегмента;

$KS_k = \{ks_{kL} \mid k = 1..M,\ L = 1..M\}$ – подмножество линий связи объектов на физическом или канальном уровнях внутри одного сегмента;

$SEG = \{X_k, G_{m+k}, KS_k \mid k = 1..N – (M + 1),\ m = 1..M\}$ – множество сетевых сегментов с линиями связи физического или канального уровня.

Объединение множеств $RVS_k = X_k \cdot KS_k \cdot G \equiv SEG$ образует модель взаимодействия объектов распределенной ВС в проекции на физический или канальный уровень модели OSI (рис. 4.1).

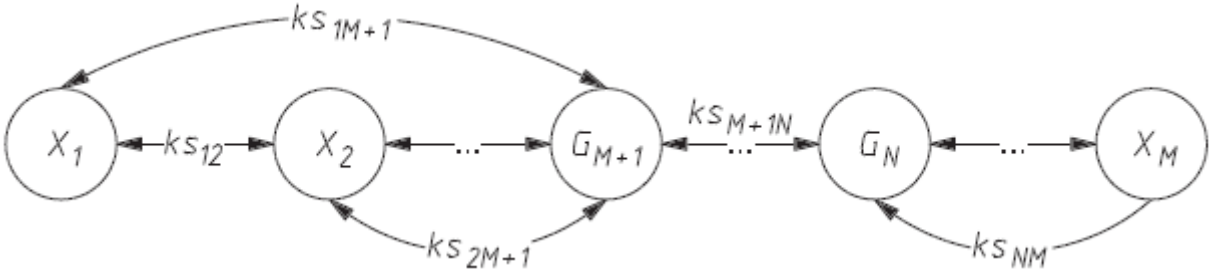


Рис. 4.1. Графовая модель взаимодействия объектов РВС в проекции на физический или канальный уровень модели OSI

Объединение множеств $RVSs = X \cdot G \cdot LS$ образует модель взаимодействия объектов распределенной ВС в проекции на сетевой уровень модели OSI (рис. 4.2).

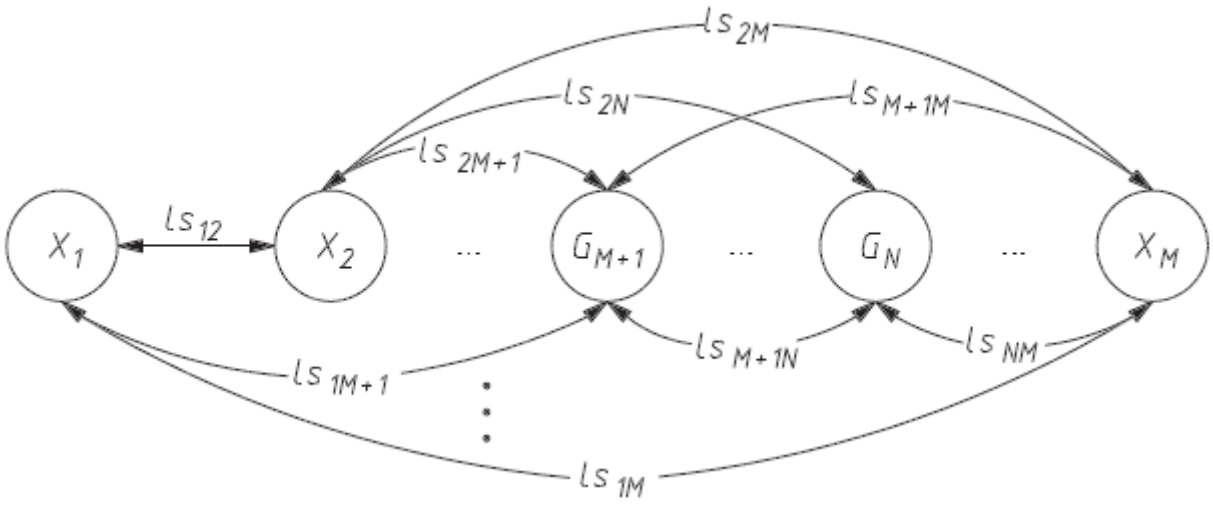


Рис. 4.2. Графовая модель взаимодействия объектов РВС в проекции на сетевой уровень

Объединение множеств RVS = RVSk . RVS_s образует модель взаимодействия объектов распределенной ВС в проекции на физический (или канальный) и сетевой уровни модели OSI (рис. 4.3).

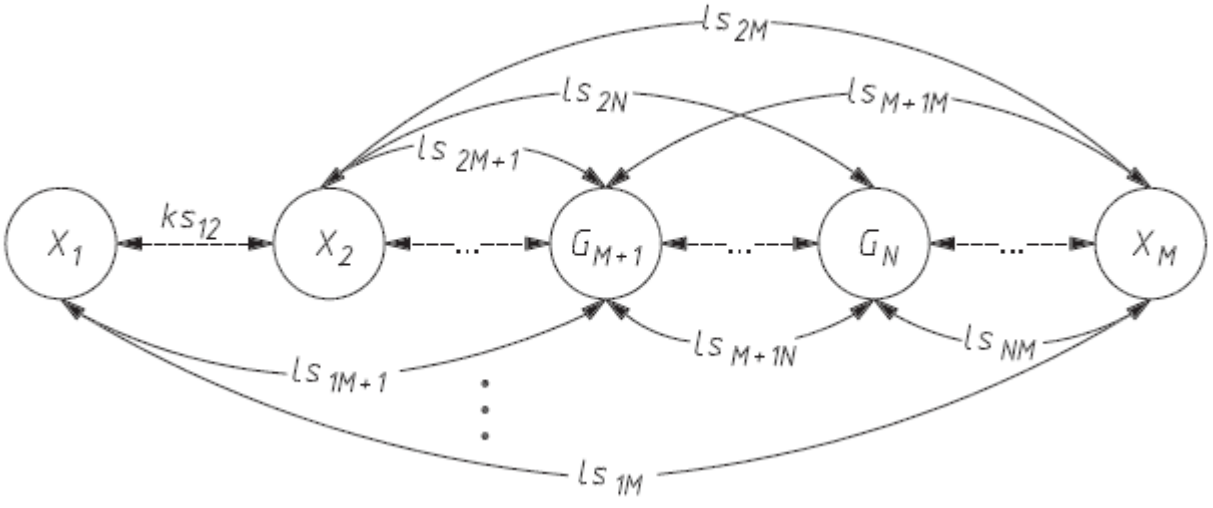


Рис. 4.3. Графовая модель взаимодействия объектов РВС в проекции на физический и сетевой уровни модели OSI

4.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Получить у преподавателя индивидуальное задание: структуру распределённой вычислительной сети и вид моделируемой угрозы информационной безопасности;

Построить графовые модели для указанных данных: обычную и реализации угрозы.

4.4. ФОРМА ОТЧЕТНОСТИ

Отчет, содержащий построенные модели, назвать по формату **ФамилияИмяОтчество_НомерГруппы_ДатаВыполненияРаботы** и поместить в папку, указанную преподавателем.

4.5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Для чего предназначена графовая модель взаимодействия объектов информационных сетей?
2. Назовите компоненты графовой модели взаимодействия объектов информационных сетей.
3. Какие виды угроз можно отобразить на графовой модели взаимодействия объектов информационных сетей?

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Internet. – М.: Издательство ДМК, 1999. – 336 с.

ЛАБОРАТОРНАЯ РАБОТА № 5. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ

5.1. ЦЕЛЬ РАБОТЫ

Целью работы является ознакомление студентов с одним из способов передачи защищаемых данных по сетям публичного доступа – построение виртуальных частных сетей.

5.2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

5.2.1. Основные положения

В литературе встречаются различные определения виртуальной частной сети (Virtual Private Network). Мы будем использовать следующее: VPN – это технология, объединяющая доверенные сети, узлы и пользователей через открытые сети, к которым нет доверия. Предположим, имеются две локальных сети (LAN-1 и LAN-2), принадлежащие одной организации (например, головной офис и филиал). Обе эти локальные сети объединены при помощи иной сети, в большинстве случаев для этого используется Интернет. С точки зрения пользователей соединения могут устанавливаться между любыми узлами этих локальных сетей. На самом же деле реальные соединения устанавливаются через посредников, неких «черных ящиков», устанавливаемых на входе в каждую из них. Задача этих «черных ящиков» так обработать идущий между ними сетевой трафик, чтобы злоумышленник или просто внешний наблюдатель не мог совершить с передаваемой информацией какого-либо действия, приводящего к ущербу. А именно, не должен нарушить конфиденциальность, целостность и подлинность информации. Иными словами, передаваемая информация, включая адреса ее получателя и отправителя, должна быть зашифрована и криптографически подписана. Кроме того, задача «черных ящиков» – защищать сами локальные сети от несанкционированного доступа к ним из глобальной сети. Таким образом, внешний наблюдатель должен увидеть в сети лишь зашифрованный обмен информацией между двумя «черными ящиками» и ничего более.

Тогда, можно сформулировать, что VPN призвана решать следующие задачи:

− обеспечивать защиту (конфиденциальность, целостность, подлинность) передаваемой по сетям информации. Как указывалось выше, данная задача решается применением криптографического метода защиты передаваемой информации;

− выполнять защиту внутренних сегментов сети от НСД извне. Решение задачи возможно благодаря встроенным в «черные ящики» функциям межсетевого экранирования, а также криптографическим механизмам, запрещающим незашифрованный сетевой трафик;

− обеспечивать идентификацию и аутентификацию пользователей. Данная задача возникает вследствие того, что, как сказано в определении VPN, в сети должны взаимодействовать лишь доверенные узлы, доверие к которым возможно после прохождения процедур идентификации и аутентификации.

Отдельно стоящей задачей, решаемой VPN, является экономия финансовых ресурсов организации, когда для обеспечения защищенной связи с филиалами применяются не защищенные выделенные каналы связи, а Интернет.

Сформулируем ряд требований, которые предъявляются к программно-аппаратным комплексам, реализующим VPN:

− масштабируемость, т. е. возможность со временем подключать новые локальные сети без необходимости изменения структуры имеющейся VPN;

− интегрируемость, т. е. возможность внедрения VPN-системы в имеющуюся технологию обмена информацией;

− легальность и стойкость используемых крипоалгоритмов, т. е. система должна иметь соответствующий сертификат, позволяющий ее использовать на территории Российской Федерации с целью защиты информации ограниченного доступа;

− пропускная способность сети, т. е. система не должна существенно увеличивать объем передаваемого трафика, а также уменьшать скорость его передачи;

− унифицируемость, т.е. возможность устанавливать защищенные соединения с другими сетями, у которых уже установлена иная VPN-система;

− общая совокупная стоимость, т. е. затраты на приобретение, развертывание и обслуживание системы не должны превосходить стоимость самой информации, особенно если речь идет о защите коммерческой тайны.

5.2.2. Туннелирование в VPN

Как указывалось выше, основная задача, решаемая VPN, – скрыть передаваемый трафик. При этом необходимо скрыть как передаваемые данные, так и адреса реальных отправителя и получателя пакетов. И кроме того, необходимо обеспечить целостность и подлинность передаваемых данных. Для защиты передаваемых данных и реальных IP-адресов применяются криптографические алгоритмы. При отправке пакетов применяется туннелирование, т.е. в пакетах, которые идут в открытой сети, в качестве адресов фигурируют только адреса «черных ящиков». Кроме того, туннелирование предполагает, что внутри локальных сетей трафик передается в открытом виде, а его защита осуществляется только тогда, когда он попадает в «туннель».

5.2.3. Уровни сетевого взаимодействия и VPN

Модель стека протоколов TCP/IP, наиболее распространённая в настоящее время, предполагает наличие четырех уровней: прикладного, транспортного, сетевого и канального. Соответственно, для каждого уровня возможность шифрования передаваемой информации различна. Так, на прикладном уровне можно скрыть данные, например, электронного письма или получаемой web-страницы. Однако факт передачи письма, т. е. диалог по протоколу SMTP скрыть невозможно. На транспортном уровне может быть вместе с данными скрыт и тип передаваемой информации, однако IP-адреса получателя и приемника остаются открытыми. На сетевом уровне уже появляется возможность скрыть и IP-адреса. Эта же возможность имеется и на канальном уровне.

Чем ниже уровень, тем легче сделать систему, функционирование которой будет незаметно для приложений высокого уровня, и тем большую часть передаваемой информации можно скрыть.

В настоящее время для каждого уровня модели стека TCP/IP разработан как минимум один протокол VPN. Так, на прикладном уровне для защиты электронной почты применяется протокол S/MIME (Secure Multipurpose Internet Mail Extension) либо система PGP. Для защиты обмена по протоколу HTTP применяется протокол SHTTP (Secure HTTP). На данном уровне шифруется текст передаваемого почтового сообщения или содержимое HTML-документа. Недостатками организации VPN на базе протоколов прикладного уровня является узкая область действия, для каждой сетевой службы должна быть своя система, способная интегрироваться в соответствующие приложения.

На транспортном уровне чаще всего применяются протоколы SSL (Secure Socket Layer) и его более новая реализация – TSL (Transport Layer Security). Также применяется протокол SOCKS. Особенность протоколов транспортного уровня – независимость от прикладного уровня, хотя чаще всего шифрование осуществляется для передачи по протоколу HTTP (режим HTTPS). Недостатком является невозможность шифрования IP-адресов и туннелирования IP-пакетов.

На сетевом уровне используются два основных протокола: SKIP (Simple Key management for Internet Protocol – простое управление ключами для IP-протокола) и IPSec. На данном уровне возможно как шифрование всего трафика, так и туннелирование, включающее скрытие IP-адресов. На сетевом уровне строятся самые распространенные VPN системы.

Канальный уровень представлен протоколами PPTP (Point-to-Point Tunneling Protocol), L2F (Layer-2 Forwarding) и L2TP (Layer-2 Tunneling Protocol). Достоинством данного уровня является прозрачность не только для приложений прикладного уровня, но и для служб сетевого и транспортного уровня. В частности, достоинством является независимость от применяемых протоколов сетевого и транспортного уровня – это может быть не только IP-протокол, но и протоколы IPX (применяется в локальных сетях с серверами на основе ОС Novell Netware) и NetBEUI (применяется в локальных сетях Microsoft). Шифрованию подлежат как передаваемые данные, так и IP-адреса.

5.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить у преподавателя индивидуальное задание: схему сети, используемый протокол организации виртуальной частной сети;
2. Используя виртуальные машины, построить схему сети;
3. Установить в виртуальных машинах программное обеспечение VPN-сервера и клиента;
4. Настроить схему виртуальной частной сети;
5. С помощью средств «прослушки» сетевого трафика проанализировать трафик в рамках доверенных и недоверенных сетей.

5.4. ФОРМА ОТЧЕТНОСТИ

Отчет, содержащий данные по анализу трафика, назвать по формату **ФамилияИмяОтчество_НомерГруппы_НомерВарианта_ДатаВыполненияРаботы** и поместить в папку, указанную преподавателем.

5.5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое VPN?
2. Для чего применяется туннелирование в VPN?
3. Каковы основные задачи, решаемые VPN?
4. Назовите протоколы VPN канального уровня.
5. В чём состоят основные недостатки протоколов VPN прикладного уровня?
6. Перечислите требования, предъявляемые к системам VPN.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. http://www.intuit.ru/department/os/winadmin/
2. http://www.intuit.ru/department/security/netsec/
3. http://www.intuit.ru/department/network/iptele/
4. Запечников С. В. Основы построения виртуальных частных сетей: Учеб. пособие для вузов / С. В. Запечников, Н. Г. Ми-

лославская, А. И. Толстой. – М.: Горячая линия–Телеком, 2003. – 249 с.

ЛАБОРАТОРНАЯ РАБОТА № 6. АНАЛИЗ СЕТЕВОГО ТРАФИКА

6.1. ЦЕЛЬ РАБОТЫ

Целью работы является приобретение студентами практических навыков анализа трафика в сети с помощью специализированных программ.

6.2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

6.2.1. Основные положения

Мониторинг и анализ сетевого трафика являются неотъемлемой частью процесса управления компьютерной сетью и используются для диагностики, тестирования и поиска неисправностей, для оптимизации структуры информационных потоков, а также выявления и решения проблем в обеспечении безопасности узлов компьютерной сети и информации, циркулирующей между ними.

Снифферы (дословный перевод – «вынюхиватели») являются специализированным ПО, предназначенным для анализа потока сообщений (трафика) вычислительной сети. Известными широкой публике (благодаря публикация в прессе в стиле «Большой Брат следит за тобой») системами подобного рода (но глобального уровня) являются ЭШЕЛОН (североамериканский проект, назначением которого является анализ содержимого линий связей Европы) и СОРМ (тотальное протоколирование трафика русскоязычной Сети).

Области применения снифферов можно разделить на:

легальные – отладка сетевого программного обеспечения, обучение, оптимизация сети (обнаружение проблем и «узких мест»), выявление несанкционированных атак на сервера Сети;

нелегальные – перехват важной информации (в первую очередь паролей и login’ов пользователей). Стандартным нелегальным приемом использования сниффера является запуск его на целевом сервере (после получения прав администратора) в скрытом режиме и несанкционированном сборе информации.

Большой проблемой современного сетевого программного обеспечения является то, что очень большое количество программ и протоколов не предусматривают вообще никакой защиты передаваемой информации. Ярким примером могут являться следующие протоколы: ICQ, POP3, telnet и т.п.

6.2.2. Методы перехвата информации

Обычно сетевая карта, работающая в сегменте **некоммутируемого** Ethernet (например, сеть построенная по спецификации 10Base-2 или 10Base-T с использованием концентраторов) в принципе «прослушивает» весь трафик своего сегмента; однако в нормальном режиме анализируются лишь первые 48 бит заголовка пакета и, если не найден собственный MAC-адрес, карта перестает читать «чужой» пакет. Функциональность сниффера достигается переводом сетевой карты в режим PROMISCUOUS MODE, обеспечивающий перехват всех сообщений, циркулирующих в данном сегменте сети безотносительно MAC-адресов.

В случае **коммутируемого** Ethernet ситуация изменяется в связи с тем, что коммутатор запоминает MAC-адреса устройств, присоединенных к конкретному порту, и не передаёт на эти порты данные, предназначенные другим узлам сети. Таким образом, перевод карты в PROMISCUOUS MODE не позволяет прослушивать «чужие» сообщения, т.к. они просто не попадают на данный порт коммутатора. В этом случае используется технология «ARP-спуфинга» (путем подделки ARP-сообщений данная сетевая карта притворяется маршрутизатором сети с MAC-адресом, однако, данной карты), при этом трафик всех составляющих сегмент сети узлов насильственно направится в сторону карты-обманщика.

6.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить у преподавателя индивидуальное задание: схему сети, используемый протокол передачи информации.
2. Используя виртуальные машины, построить схему сети.
3. Установить в виртуальных машинах программное обеспечение сниффера и протокола передачи информации.

4. С помощью сниффера проанализировать сетевой трафик на возможность извлечения учетных данных пользователей и информации.

6.4. ФОРМА ОТЧЕТНОСТИ

Отчет, содержащий данные по анализу трафика, назвать по формату **ФамилияИмяОтчество_НомерГруппы_НомерВарианта_ДатаВыполненияРаботы** и поместить в папку, указанную преподавателем.

6.5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что представляет из себя ПО класса снифферов и с какими целями применяется?
2. Каковы ограничения методов перехвата информации снифферами?
3. Какие методы применяют с целью исключения возможности перехвата информации снифферами?

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. http://intelsys.ucoz.ru/lab_issledovanie_setevykh_protokolov.pdf
2. http://www.4stud.info/networking/work2.html
3. http://www.intuit.ru/department/internet/iissecurity/
4. http://www.intuit.ru/department/network/baslocnet/

ЛАБОРАТОРНАЯ РАБОТА № 7. МЕТОДЫ СКАНИРОВАНИЯ ПОРТОВ

7.1. ЦЕЛЬ РАБОТЫ

Целью работы является ознакомление студентов с методами поиска открытых портов на сетевых узлах, приобретение практических навыков работы со сканером портов.

7.2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

7.2.1. Основные положения

Сканированием портов называется процесс исследования узлов сети на наличие открытых для соединения портов. Поскольку типичным взаимодействием с серверной частью сетевого программного обеспечения является посылка данных на открытый для соединения порт (с возможным последующим переключением на другой порт), то наличие открытых для соединения портов говорит о том, что на узле запущена какая-либо сетевая служба. С целью обеспечения работы разнородных узлов в сети часть портов зарезервировано для работы строго определённых служб (так называемые well-known ports), например, TCP порт 80 соответствует web-серверу, TCP порт 25 – почтовому серверу. Процесс сканирования портов может использоваться злоумышленниками с целью реализации угрозы раскрытия параметров системы.

Сканером портов называется программно-аппаратный комплекс, предназначенный для реализации процесса сканирования портов. Возможности сканеров портов довольно сильно отличаются вследствие различий программного обеспечения. Одним из наиболее известных и функциональных сканеров портов является свободная программа nmap, разработанная Гордоном Лионом (Gordon Lyon). Nmap предназначен для сканирования сетей с любым количеством узлов, определения состояния объектов сканируемой сети, портов и соответствующих им служб, определения операционной системы узлов сети (с использованием «отпечат-

ков пальцев TCP/IP»), определения наличия межсетевых экранов. Nmap поддерживает следующие методы сканирования портов.

7.2.2. Методы сканирования

Наиболее общим (и «стандратным») методом сканирования TCP портов является **TCP connect**. Функция connect(), присутствующая в любой ОС, позволяет создать соединение с любым портом удаленной машины. Если указанный в качестве аргумента порт открыт и прослушивается сканируемой машиной, то результат выполнения connect() будет успешным (т.е. соединение будет установлено), в противном случае указанный порт является закрытым, либо доступ к нему заблокирован средствами защиты.

Для того, чтобы использовать данный метод, пользователь может не иметь никаких привилегий на сканирующем хосте. Этот метод сканирования легко обнаруживается целевым (т.е. сканируемым) хостом, поскольку его log-файл будет содержать запротоколированные многочисленные попытки соединения и ошибки выполнения данной операции. Службы, выполняющие обнаружение попыток сканирования портов, немедленно заблокируют доступ адресу, вызвавшему эти ошибки.

Метод «полуоткрытого» сканирования или **TCP SYN** – при этом способе полное TCP-соединение с портом сканируемой машины не устанавливается. Nmap посылает SYN-пакет, как бы намереваясь открыть настоящее соединение, и ожидает ответ. Наличие флагов SYN|ACK в ответе указывает на то, что порт удаленной машины открыт и прослушивается. Флаг RST в ответе означает обратное. Если nmap принял пакет SYN|ACK, то в ответ немедленно отправляет RST-пакет для сброса еще не установленного соединения (реально эту операцию выполняет сама ОС). Пользователь должен иметь статус администратора для формирования поддельного SYN-пакета.

Методы **FIN, Xmas Tree и NULL**-сканирования используются в случае, если SYN-сканирование по каким-либо причинам оказалось неработоспособным. Так, некоторые межсетевые экраны и пакетные фильтры «ожидают» поддельные SYN-пакеты на защищенные ими порты, и программы типа Synlogger или

Courtney способны отследить SYN-сканирование. Идея заключается в следующем. В FIN-сканировании в качестве запроса используется пакет с установленным флагом FIN. В Xmas Tree используется пакет с набором флагов FIN|URG|PSH, а NULL-сканирование использует пакет без флагов. Согласно рекомендации RFC 973, ОС сканируемого хоста должна ответить на такой пакет, прибывший на закрытый порт, пакетом RST, в то время как открытый порт должен игнорировать эти пакеты. Разработчики Microsoft Windows, как обычно, решили полностью игнорировать все общепринятые стандарты и пойти своим путем. Поэтому любая ОС семейства Windows не посылает в ответ RST-пакет, и данные методы не будут работать с этими ОС. Однако в nmap этот признак является основным для различения операционных систем, обладающих таким свойством. Если в результате FIN-сканирования получили список открытых портов, то это не Windows. Если же все эти методы выдали результат, что все порты закрыты, а SYN-сканирование обнаружило открытые порты, то скорей всего на узле работает ОС Windows.

В ряде случаев необходимо лишь узнать адреса активных хостов в сканируемой сети. Nmap может сделать это, используя **ping сканирование**, послав ICMP-сообщение echo-request на каждый указанный IP-адрес. Хост, отправивший ответ на эхо, является активным. Некоторые сайты (например, microsoft.com) блокируют эхо-пакеты. По этой причине nmap также посылает TCP ACK-пакет на 80-й порт сканируемого хоста (по умолчанию). Если в ответ вы получили RST-пакет, хост активен. Третий метод использует SYN-пакет и ожидает в ответ RST либо SYN|ACK. Для пользователей, не обладающих статусом администратора, используется метод connect(). Для пользователей с полномочиями администратора nmap по умолчанию использует параллельно оба метода – ICMP и ACK. Заметим, что ping-сканирование по умолчанию выполняется в любом случае и только активные хосты подвергаются сканированию.

Для определения открытых UDP портов на исследуемом узле используется **UDP сканирование**. На каждый порт сканируемой машины отправляется UDP-пакет без данных. Если в ответ было получено ICMP-сообщение «порт недоступен» (port unreachable), это означает, что порт закрыт. Если на посланный

UDP-пакет получен ответ, считается, что сканируемый порт открыт. Если на запрос не получено никаких ответов, то состояние порта будет «opened|filtered», что означает, что порт либо открыт, либо пакетные фильтры блокируют обмен данными. В данном случае можно провести дополнительные тесты для определения истинного состояния UDP порта.

Для определения IP-протоколов, поддерживаемых сканируемым узлом используется сканирование **протоколов IP**. Метод заключается в передаче хосту IP-пакетов без какого-либо заголовка для каждого протокола сканируемого хоста. Если получено сообщение «протокол недоступен» (protocol unreachable), то данный протокол хостом не используется. В противном случае nmap предполагает, что протокол поддерживается хостом. Некоторые ОС и межсетевые экраны могут блокировать передачу сообщений «протокол недоступен». По этой причине все сканируемые протоколы будут «открыты» (т.е. поддерживаются).

Сканирование с помощью промежуточного узла позволяет произвести абсолютно невидимое сканирование портов. Атакующий может просканировать цель, не посылая при этом пакетов от своего IP-адреса. Вместо этого используется метод idle scan (открытый в 1998 году), позволяющий просканировать жертву через промежуточный узел (называемый узел-«зомби»). Кроме абсолютной невидимости машины, выполняющей сканирование, этот тип сканирования позволяет определить политику доверия между машинами на уровне протокола IP. Листинг результатов показывает открытые порты со стороны хоста-«зомби». Таким образом, можно просканировать цель с использованием нескольких «зомби», которым цель может «доверять», в обход межсетевых экранов и пакетных фильтров.

Дополнительный метод **ACK-сканирования** используется для определения набора правил межсетевого экрана. В частности, он помогает определить, защищен ли сканируемый хост межсетевым экраном или просто пакетным фильтром, блокирующим входящие SYN-пакеты. В этом методе на сканируемый порт хоста отправляется ACK-пакет (со случайными значениями полей acknowledgement number и sequence number). Если в ответ пришел RST-пакет, порт классифицируется как «нефильтруемый». Если ответа не последовало (или пришло ICMP-сообщение о недос-

тупности порта), порт классифицируется как «фильтруемый». Обратите внимание, что этот метод никогда не покажет состояние порта «открыт» в результатах сканирования.

7.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить у преподавателя индивидуальное задание: схему сети, используемые типы сканирования.
2. Используя виртуальные машины, построить схему сети.
3. С помощью утилиты nmap провести сканирование узлов виртуальной сети.
4. Изменить настройки межсетевых экранов на узлах виртуальной сети, выполнить сканирование с помощью nmap ещё раз.

7.4. ФОРМА ОТЧЕТНОСТИ

Отчет, содержащий данные с результатами работы nmap, назвать по формату **ФамилияИмяОтчество_НомерГруппы_НомерВарианта_ДатаВыполненияРаботы** и поместить в папку, указанную преподавателем.

7.5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое сканер портов?
2. Какие угрозы безопасности реализуются процессом сканирования портов?
3. Чем опасен метод сканирования портов с использованием промежуточного узла?
4. Какие хорошо известные порты сетевых служб Вы знаете?

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. http://nmap.org/

ЛАБОРАТОРНАЯ РАБОТА № 8. КОНФИГУРИРОВАНИЕ МЕЖСЕТЕВЫХ ЭКРАНОВ

8.1. ЦЕЛЬ РАБОТЫ

Целью работы является ознакомление студентов со средствами защиты узлов сети от нежелательного трафика.

8.2. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

8.2.1. Основные положения

Межсетевой экран (МЭ) – это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или исходящей из нее.

МЭ повышает безопасность объектов внутренней сети за счет игнорирования несанкционированных запросов из внешней среды. Это уменьшает уязвимость внутренних объектов, так как сторонний нарушитель должен преодолеть некоторый защитный барьер, в котором механизмы обеспечения безопасности сконфигурированы особо тщательно. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Кроме того, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что способствует поддержанию во внутренней области режима конфиденциальности. Кроме функций разграничения доступа, МЭ может обеспечивать выполнение дополнительных функций безопасности (аутентификацию, контроль целостности, фильтрацию содержимого, обнаружение атак, регистрацию событий).

МЭ не является симметричным устройством, для него определены понятия «внутри» и «снаружи» (входящий и исходящий трафики). При этом задача экранирования формулируется как

защита внутренней области от неконтролируемой и потенциально враждебной внешней.

8.2.2. Компоненты межсетевого экрана

В общем случае алгоритм функционирования МЭ сводится к выполнению двух групп функций, одна из которых ограничивает перемещение данных (фильтрация информационных потоков), а вторая, наоборот, ему способствует (посредничество в межсетевом взаимодействии). Следует отметить, что выполнение МЭ указанных групп функций может осуществляться на разных уровнях модели OSI. Принято считать, что чем выше уровень модели OSI, на котором МЭ обрабатывает пакеты, тем выше обеспечиваемый им уровень защиты.

Как отмечено выше, МЭ может обеспечивать защиту АС за счет фильтрации проходящих через него сетевых пакетов, то есть посредством анализа содержимого пакета по совокупности критериев на основе заданных правил и принятия решения о его дальнейшем распространении в (из) АС. Таким образом, МЭ реализует разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного типа между субъектами и объектами. Как следствие, субъекты одной АС получают доступ только к разрешенным информационным объектам другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр. МЭ или один из его компонентов, функционирующий вышеописанным образом, называют пакетным фильтром.

8.2.3. Политика межсетевого экранирования

При настройке политики межсетевого экранирования рассматривают два аспекта сетевой безопасности: политику доступа к сетевым ресурсам и политику реализации собственно МЭ. Политика доступа к сетевым ресурсам отражает общие требования по безопасности той или иной организации, и при ее разработке

должны быть сформулированы правила доступа пользователей к различным сервисам, используемым в организации. Указанные правила описывают, какой внутренний (внешний) пользователь (группа пользователей), когда, с какого внутреннего (внешнего) узла сети и каким сервисом может воспользоваться с уточнением в случае необходимости способов аутентификации пользователей и адресов целевых серверов.

Политика реализации МЭ определяет, каким образом применяется политика доступа к сетевым ресурсам, и в ряде случаев зависит от используемых сервисов и выбранных средств построения экрана. Как правило, при выборе политики реализации МЭ останавливаются на одной из двух базовых стратегий:

− разрешать все, что явно не запрещено;

− запрещать все, что явно не разрешено.

Хотя может показаться, что эти две стратегии очень просты и почти не отличаются друг от друга, на самом деле это не так. При выборе первой стратегии МЭ по умолчанию разрешает все сервисы, которые не указаны как запрещенные. В этом случае для обеспечения безопасности сети придется создавать правила, которые учитывали бы все возможные запреты. Это не только приведет к необходимости описания большого количества правил, но и заставит пересматривать их при появлении каждого нового протокола или сервиса, которые существующими правилами не охватываются.

Вторая стратегия строже и безопаснее. Намного проще управлять МЭ, запретив весь трафик по умолчанию и задав правила, разрешающие прохождение через границу сети только необходимых протоколов и сервисов. Запрет всего трафика по умолчанию обеспечивается вводом правила «Запрещено все» в последней строке таблицы фильтрации. Однако в ряде случаев, в частности при использовании простого пакетного фильтра, описание правил допустимых сервисов также сопряжено с трудоемким процессом, требующим досконального знания алгоритмов функционирования протоколов в рамках того или иного сервиса.

Учитывая взрывной рост угроз в сети Интернет в последнее время, использование первой стратегии видится совершенно бессмысленным.

8.3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить у преподавателя индивидуальное задание: схему сети, разрешённый к прохождению трафик.
2. Используя виртуальные машины, построить схему сети.
3. С помощью программного обеспечения межсетевого экрана установить политику «запрещено всё, что явно не разрешено».
4. Используя стандартные утилиты диагностики сети, сканер портов и другое сетевое программное обеспечение убедиться в действенности установленной политики.
5. Внести в конфигурацию межсетевого экрана изменения в соответствии с индивидуальным заданием.
6. Используя сетевое программное обеспечение убедиться в работоспособности сделанных настроек.

8.4. ФОРМА ОТЧЕТНОСТИ

Отчет, содержащий данные с результатами работы средств диагностики сети для обеих случаев, назвать по формату **ФамилияИмяОтчество_НомерГруппы_НомерВарианта_ДатаВыполненияРаботы** и поместить в папку, указанную преподавателем.

8.5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие типы межсетевых экранов Вы знаете?
2. Объясните разницу между statefull и stateless межсетевым экраном.
3. Какие политики межсетевых экранов Вы знаете?
4. Каков порядок проверки правил межсетевых экранов?

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. http://www.intuit.ru/department/network/firewalls.
2. Роберт Л. Зиглер. Брандмауэры в Linux. – М.: Издательский дом «Вильямс», 2000. – 384 с.

ОГЛАВЛЕНИЕ