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

Кафедра сетей и устройств телекоммуникаций

ПАРОЛЬНЫЕ МЕТОДЫ ОПОЗНАНИЯ В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ

Методические указания
к лабораторной работе

по дисциплине «Защита программного обеспечения
и баз данных в сетях телекоммуникаций»
для студентов специальностей I-45 01 03 «Сети телекоммуникаций»
и I-98 01 02 «Защита информации в телекоммуникациях»
всех форм обучения

Минск 2008

УДК 621.391.25(075.8)
ББК 32.811 я73
П 18

Составители:
М.Н. Бобов, П. М. Буй

Парольные методы опознания в сетях телекоммуникаций : метод. указания к лаб. работе по дисц. «Защита программного обеспечения и баз данных в сетях телекоммуникаций» для студ. спец. I-45 01 03 «Сети телекоммуникаций» и I-98 01 02 «Защита информации в телекоммуникациях» всех форм обуч. / сост. М. Н. Бобов, П. М. Буй. – Минск : БГУИР, 2008. – 26 с.

П 18

Исследуются методы опознания субъектов с использованием паролей в сетях телекоммуникаций. Рассматриваются принципы повышения защищенности парольных методов опознания.

Лабораторная работа может быть использована при изучении других курсов, связанных с защитой программного обеспечения и баз данных в сетях телекоммуникаций.

УДК 621.391.25(075.8)
ББК 32.811 я73

1. Цель лабораторной работы

Изучение парольных систем опознания в сетях телекоммуникаций.

2. Теоретические сведения

Реализация процедур опознания, которые включают в себя идентификацию и аутентификацию, является общей проблемой для любых систем, в которых требуется обеспечивать разграничение доступа к обрабатываемой информации.

Функционирование всех механизмов разграничения доступа, использующих аппаратные или программные средства, основано на предположении, что любой субъект системы представляет собой конкретное лицо. Следовательно, существует некоторый механизм, обеспечивающий установление подлинности субъекта, обращающегося к системе. Идентификация – это процесс распознавания субъекта с помощью заранее присвоенного идентификатора. Аутентификация – это процесс, заключающийся в проверке подлинности субъекта.

В общем случае существуют три класса опознания, которые базируются на:

а) условных, заранее присваиваемых признаках (сведениях), известных субъекту (что знает субъект);

б) физических средствах, действующих аналогично физическому ключу (что имеет субъект);

в) индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц (что присуще субъекту).

Парольные системы опознания в той или иной степени используются в первых двух классах опознания. Рассмотрим эти классы подробнее.

2.1. Описание методов опознания на основе принципа «что знает субъект»

Существующие парольные методы проверки подлинности субъектов при входе в систему можно разделить на две группы:

– методы проверки подлинности на основе простого пароля;

– методы проверки подлинности на основе динамически изменяющегося пароля.

При использовании метода простого пароля его значение не изменяется в течение установленного администратором службы безопасности времени действия.

При использовании динамически изменяющегося пароля его значение для каждого нового сеанса работы изменяется по определённым правилам.

Метод простых паролей заключается в том, что субъект на клавиатуре пульта ввода данных или на специально имеющемся наборном поле набирает только ему известную комбинацию букв и цифр, являющуюся, собственно, паролем. Данный пароль сравнивается с эталонным, хранящимся в системе, и при положительном результате проверки субъект получает доступ к системе. Данная схема опознания является простой с точки зрения реализации, т.к. не требует никакой специальной аппаратуры и реализуется посредством небольшого объема программного обеспечения.

Схема с простым паролем имеет два недостатка:

– сложность запоминания для большинства субъектов произвольного набора символов, используемого в качестве пароля;

– уязвимость пароля при наборе, т.к. его значение можно подсмотреть.

Модернизацией схемы простого пароля является схема паролей однократного использования. В этой схеме субъекту выдается список из N паролей. Такие же N паролей хранятся в системе. Здесь при каждом обращении к системе синхронно используется пароль с текущим номером, а все пароли с предыдущими номерами вычеркиваются. В случае если старый пароль из предыдущего сеанса стал известен другому субъекту, система его не воспринимает, т.к. действующим будет следующий по списку пароль. Данная схема обеспечивает большую степень безопасности, но она является и более сложной.

Схема паролей однократного использования имеет следующие недостатки:

– субъект должен помнить или иметь при себе весь список паролей и следить за текущим паролем;

– в случае, если встречается ошибка в процессе передачи, трудно определить, следует ли передавать тот же самый пароль или послать следующий;

– необходимо иметь разные таблицы паролей для каждого субъекта, т.к. может произойти рассинхронизация работы.

Последний недостаток можно устранить, используя так называемый генератор паролей. Его применение избавляет от необходимости хранить таблицы па-

ролей для каждого субъекта, однако первые два недостатка данной схемы сохраняются.

Методы проверки подлинности на основе динамически изменяющегося пароля обеспечивают большую безопасность, т.к. частота смены паролей в них максимальна – пароль для каждого субъекта меняется ежедневно или через несколько дней. При этом каждый следующий пароль по отношению к предыдущему изменяется по правилам, зависящим от используемого метода проверки подлинности.

Существуют следующие методы парольной защиты, основанные на использовании динамически изменяющегося пароля:

– методы модификации схемы простых паролей;
– метод «запрос–ответ»;
– функциональные методы.

К методам модификации схемы простых паролей относят случайную выборку символов пароля и одноразовое использование паролей.

При использовании первого метода каждому субъекту выделяется достаточно длинный пароль, причем каждый раз для опознавания используется не весь пароль, а только его некоторая часть. В процессе проверки подлинности система запрашивает у субъекта группу символов по заданным порядковым номерам. Количество символов и их порядковые номера для запроса определяются с помощью датчика псевдослучайных чисел.

При одноразовом использовании паролей каждому субъекту выделяется список паролей. В процессе запроса номер пароля, который необходимо ввести, выбирается последовательно по списку или по схеме случайной выборки.

Недостатком методов модификации схемы простых паролей является необходимость запоминания субъектами длинных паролей или их списков. Запись же паролей на бумагу или в записные книжки приводит к появлению риска потери или хищения носителей информации с записанными на них паролями.

При использовании метода «запрос–ответ» заблаговременно создается и особо защищается массив вопросов, включающий в себя как вопросы общего характера, так и персональные вопросы, относящиеся к конкретному субъекту, например, вопросы, касающиеся известных только субъекту сведений из его жизни.

В методе «запрос–ответ» набор ответов на m стандартных и n ориентированных на субъекта вопросов хранится в ЭВМ и управляет программой опознания. Когда субъект делает попытку включиться в работу, программа опознания случайным образом выбирает и задает ему некоторые (или все) из этих вопросов. Субъект должен дать правильный ответ на все вопросы, чтобы получить разрешение на доступ к системе. Вопросы могут быть выбраны таким образом, чтобы субъект запомнил ответы и не записывал их.

Основным требованием к вопросам в данном методе аутентификации является уникальность, подразумевающая, что правильные ответы на вопросы знают только субъекты, для которых эти вопросы предназначены.

Модификация этого метода предполагает изменение каждый раз одного или более вопросов, на которые субъект давал ответ до того.

Существует два варианта использования метода «запрос–ответ», вытекающие из условий $m = 0$ или $n = 0$. Вариант с $m = 0$ предполагает, что вопросы составлены на основе различных фактов биографии индивидуального субъекта, представляют собой имена его друзей, дальних родственников, старые адреса и т.д. На опознавательный вопрос субъект, который его сам предложил, всегда даст правильный ответ, что не сможет сделать злоумышленник.

Иногда предпочтительнее вариант с $n = 0$, т.е. субъектам задается большее количество стандартных вопросов и от них требуются ответы на те, которые они сами выберут. Достоинство рассмотренной схемы в том, что субъект может выбирать вопросы, а это дает весьма хорошую степень безопасности в процессе включения в работу. В то же время нет необходимости хранить в системе тексты вопросов для каждого субъекта, достаточно хранить указатели на вопросы, выбранные данным субъектом, вместе с информацией, устанавливающей его подлинность. Текст каждого стандартного вопроса необходимо ввести для хранения только один раз, поэтому в системе с большим числом субъектов это может дать экономию памяти.

Метод «запрос–ответ» наряду с достоинствами все же имеет недостатки, ограничивающие возможность его использования. Во-первых, он требует проявления изобретательности со стороны самих субъектов, что для них является дополнительной нагрузкой. Во-вторых, для большинства людей опознавательные вопросы и ответы, как правило, приобретают стереотипность, и весьма вероятно, что настойчивый нарушитель может, собрав статистику, подготовиться по мно-

гим вопросам. В-третьих, метод требует обмена множеством опознавательных запросов и соответствующих им ответов, что для субъектов является сложным и утомительным. Кроме того, в силу его некоторой громоздкости метод «запрос–ответ» может удачно использоваться только для небольших организованных групп субъектов и не применим для массового использования.

Среди функциональных методов наиболее распространенными являются метод функционального преобразования пароля, а также метод «рукопожатия».

В процессе «рукопожатия» субъект должен обменяться с алгоритмом последовательностью паролей (команд), которые должны быть названы правильно и в правильной последовательности, хотя сам субъект не знает алгоритма. Правильное завершение алгоритма подтверждает подлинность субъекта.

Метод функционального преобразования основан на использовании некоторой функции *F*, которая должна удовлетворять следующим требованиям:

– для заданного числа или слова *X* легко вычислить $Y = FA(X)$;

– зная *X* и *Y*, сложно или невозможно определить функцию $Y = FA(X)$.

Необходимым условием выполнения данных требований является наличие в функции $FA(X)$ динамически изменяющихся параметров, например, текущих даты, времени, номера дня недели или возраста субъекта.

Метод «рукопожатия» заключается в следующем. Для установления подлинности система выдает субъекту число, выбранное случайным образом, а затем запрашивает от него ответ. Для подготовки ответа субъект *A* применяет собственное, заранее подготовленное преобразование F_A. Информацией, на основе которой принимается решение, здесь является не пароль, а преобразование F_A. ЭВМ посылает значение *X*, а субъект отвечает значением $F_A(X)$. Любое постороннее лицо для проникновения в систему даже в случае знания значений *X* и $F_A(X)$ должно тем не менее отгадать функцию преобразования на основе нескольких вводов и выводов, т.к. сама функция преобразования никогда не передается по линиям связи, по которым посылается только *X* и $F_A(X)$. Функция преобразования может быть различной для каждого субъекта, что позволяет однозначно идентифицировать каждое лицо, обращающееся к системе.

С целью достижения высокого уровня безопасности функция преобразования пароля, задаваемая для каждого субъекта, должна периодически меняться. Для высокой безопасности функцию «рукопожатия» целесообразно циклически менять через определенные интервалы времени.

Достоинством метода «рукопожатия» является то, что никакой конфиденциальной информации между субъектом и системой не передается. По этой причине эффективность данного метода особенно велика при его применении в вычислительных сетях для подтверждения подлинности субъектов, пытающихся осуществить доступ к серверам или центральным ЭВМ.

В некоторых случаях может оказаться необходимым субъекту проверить подлинность той ЭВМ, к которой он хочет осуществить доступ. Необходимость во взаимной проверке может понадобиться и когда два субъекта хотят связаться друг с другом по линии связи. Методы простых паролей, а также методы модификации схем простых паролей в этом случае не подходят. Наиболее подходящим здесь является метод «рукопожатия». При его использовании ни один из участников сеанса связи не будет получать никакой секретной информации.

Способ «рукопожатия» более труден для раскрытия, чем пароль, но сложнее в реализации. В отличие от паролей преобразование никогда не появляется в линиях связи, однако в силу своей неизменности также может быть достаточно просто определено. Основным недостатком метода «рукопожатия» является временная задержка, выражающаяся в необходимости, как в методе «запрос–ответ», организации обмена несколькими сообщениями между субъектом и системой в процессе опознания.

2.2. Описание методов опознания на основе принципа «что имеет субъект»

К этому классу опознания относятся методы, основывающиеся на физических средствах, которые имеет при себе данный субъект, обращающийся к системе.

К ним относятся идентификационные карты с перфорированным или магнитным кодом, а также ряд активных устройств, называемых электронными ключами, включающих в себя: смарт-карты с процессорами, USB-брелоки, устройства Touch Memory и прочие подобные технические средства.

В магнитных картах информация записывается на нескольких дорожках магнитного слоя и представляет собой данные, используемые для идентификации. К этим данным относятся: номер субъекта или его имя, пароль, количество допустимых использований карты и т.д. Наряду с очевидной простотой использования магнитные карты обладают низкой защищенностью от копирования со-

держимого. Для защиты от копирования магнитные карты снабжаются различными защитными средствами. Один из методов состоит в нанесении магнитного слоя обычного типа поверх второго слоя с более высокой коэрцитивной силой, т.е. для изменения состояния того слоя требуется более сильное магнитное поле. Тогда обычными методами невозможно считать или изменить запись нижнего слоя. Считывающее устройство, читая карту, содержащую идентификатор, вначале создает поле, стирающее любую запись, сделанную обычным способом, а затем уже считывает лежащую ниже «твердую» запись, в которой действительно находится информация.

Другой метод использует постоянную магнитную разметку ленты, которая наносится в процессе ее производства. Метод, известный под названием «влажной разметки», состоит в определенной ориентации осей ферромагнитных кристаллов, пока наполнитель еще не высох, причем селективная ориентация осей кристаллов в различных частях ленты создает магнитную запись, которую никак нельзя изменить.

Чтобы прочесть эту запись, кристаллы необходимо подвергнуть воздействию постоянного магнитного поля с определенной ориентацией. Изменение положения кристаллов вдоль ленты будет наводить внешнее поле, которое можно прочитать с помощью обычных удобно расположенных головок. Изготовленные таким образом идентификационные карточки могут обеспечить «уникальную» идентичность, которую трудно подделать, поскольку для этого требуется овладеть технологией производства магнитных покрытий и влажной разметки.

Ясно, что для осуществления защиты от подделки или копирования карточки требуют сложной технологии их изготовления и, соответственно, сложной аппаратуры для считывания записанной на них информации. Следует отметить, что при любых способах достичь абсолютной защиты от копирования магнитных карт практически невозможно, т.к. носитель всегда открыт для доступа посторонних лиц.

Электронный ключ в самом общем смысле представляет собой физический носитель идентификатора субъекта, его пароля. В отличие от парольных систем при использовании электронного ключа субъект имеет ряд преимуществ:

– ему не надо запоминать значение пароля, т.к. пароль записан в ключе;

– он освобожден от функции защиты пароля от компрометации при его вводе, т.к. пароль считывается из ключа;

– все функции по защите от подделки пароля или его несанкционированного использования (метод разовых паролей, метод «рукопожатия») возлагаются на электронный ключ;

– идентификатор можно сделать сколь угодно большим, т.к. субъект с ним не работает.

В силу того что, как и идентификационная магнитная карта, электронный ключ является физическим средством хранения идентификатора субъекта, его можно скопировать и подделать. В основном все многообразие электронных ключей и классифицируется по основному признаку, определяющему их защищенность от копирования и подделки, т.к. быстродействие, объем хранимого идентификатора, габариты и другие характеристики являются, по существу, производными от него.

Ключ, который невозможно подделать, является активным устройством, содержащим в памяти идентификатор, не доступный для чтения. Например, электронный ключ может содержать криптосхему, в которую при изготовлении загружается случайное значение ключа. Вне криптосхемы это значение нигде не записывается. Устройство можно сконструировать таким образом, что попытка прочесть ключ приводит к его уничтожению. Устройство такого типа обладает «индивидуальностью», которую можно выявить только посредством задания устройству различных цифровых значений и записи его ответов.

Электронный ключ может использоваться локально, подобно ключу от дверного замка, или на расстоянии, например, для идентификации удаленных субъектов, обращающихся к ЭВМ. Для своего восприятия электронный ключ должен иметь «замок» (ответную часть), запрашивающий ключ и проверяющий его идентичность. Вначале идентичность необходимо определить каким-либо независимым способом, чтобы ввести в действие замок, отвечающий данному ключу. Затем замок посылает набор запросов к ключу и запоминает его ответы. Впоследствии, когда ключ действительно используется для опознания субъекта, некоторые из этих наборов повторяются в качестве опознавательных вопросов к ключу, а ответы сравниваются с уже хранящимися в памяти. Если опознание осуществляется многократно, то замок может послать новые цифровые комбинации, которые добавляются к списку опознавательных вопросов и ответов. Например, для своего восприятия смарт-карта должна иметь ридер, в процессе обмена информацией с которым происходит опознание смарт-карты.

Опознание субъекта происходит после подтверждения им того, что именно он является владельцем смарт-карты в результате ввода с клавиатуры PIN-кода. Аналогом ридера для USB-ключей выступает стандартный USB-порт, а для электронного ключа Touch Memory – считывающее устройство.

Один и тот же ключ может подходить к нескольким замкам, и один и тот же замок может отвечать нескольким ключам, не нарушая при этом секретности ни замка, ни ключа. Никакие исследования такого физического замка не позволят определить хранящийся ключ, если он защищен эффективной криптосхемой. Однако если имеется возможность перехвата всех опознавательных вопросов и ответов для данного замка, то ключ можно подделать. Такой поддельный ключ может приниматься за подлинный во всех последующих сеансах опознания до тех пор, пока он не будет выявлен новыми опознавательными вопросами. Используя большое число ответов и создавая каждый раз новые, можно повысить уровень защиты, однако более надежным способом является применение методов шифрования для защиты передаваемых идентификаторов от удаленных абонентов в ЭВМ.

2.3. Принципы, повышающие стойкость парольных методов опознания

Стойкость парольных средств опознания определяется вероятностью подбора с пароля или PIN-кода.

Для повышения эффективности этих средств при их проектировании необходимо использовать следующие принципы:

– принцип максимального правдоподобия;

– принцип ограничения попыток;

– принцип цикличности.

Принцип максимального правдоподобия заключается в следующем. Пусть $A = \{a_i\}$, $i = 1, n$ – эталонные значения параметров, используемых для аутентификации, а $X = \{x_i\}$, $i = 1, n$ – значения параметров, предъявляемых для опознания.

Пусть независимые попытки опознания имеют частные вероятности $\rho(X,A)$, тогда принцип максимального правдоподобия состоит в выборе в качестве истинного такого параметра X, при котором максимизируется функция правдоподобия:

$$L(q) = r(x_1, a_1), r(x_2, a_2) \mathbf{K}\, r(x_n, a_n).$$

Для средств опознания, основанных на том, «что знает субъект» и «что имеет субъект», принцип максимального правдоподобия заключается в том, что опознание считается успешным при абсолютном совпадении всех сравниваемых признаков входного воздействия, предоставленного субъектом, и эталонного, хранящегося в памяти средства опознания. Это обусловлено тем, что результат преобразования признаков, предоставляемых одним и тем же субъектом, в понятный средству опознания вид всегда имеет одинаковые значения.

В этом случае вероятность подбора пароля с первой попытки определяется по формуле:

$$P_1 = \frac{1}{N}, \tag{1}$$

где P_1 – вероятность подбора пароля с первой попытки;

N – объем алфавита.

Для паролей объем алфавита вычисляется следующим образом:

$$N = A^n, \tag{2}$$

где A – используемый алфавит пароля (общее число знаков);

n – длина пароля.

Тогда

$$P_1 = \frac{1}{A^n}. \tag{3}$$

В средствах опознания с использованием смарт-карт субъект предоставляет PIN-код, состоящий из цифр. Поэтому алфавит PIN-кода равен десяти. Для этих средств опознания формула определения вероятности подбора PIN-кода с первой попытки имеет следующий вид:

$$P_1 = \frac{1}{10^n}. \tag{4}$$

В средствах опознания с использованием электронных ключей или брелоков используются битовые ключи, поэтому алфавит ключей равен двум. Формула определения вероятности подбора битового ключа с первой попытки имеет вид

$$P_1 = \frac{1}{2^n}. \tag{5}$$

Вероятность подбора пароля с первой попытки при неповторяющихся символах в пароле определяется по следующей формуле:

$$P_{1\text{неповт}} = \prod_{i=0}^{n-1} \frac{1}{N-i}, \tag{6}$$

где $P_{1\text{неповт}}$ – вероятность подбора пароля с первой попытки при неповторяющихся символах в пароле.

В данном случае количество символов не может быть больше алфавита.

Увеличение вероятности правильного опознания субъекта для данных средств опознания достигается за счет расширения алфавита или длины пароля.

Принцип ограничения попыток заключается в том, что при опознании субъекта ограничивается число попыток неправильного входа в систему.

При отсутствии ограничения на число попыток неправильного входа значение вероятности подбора пароля определяется по формуле

$$P_{\text{ПП}} = P_{\text{ПП1}} + (1 - P_{\text{ПП1}}) \cdot P_{\text{ПП2}} + (1 - P_{\text{ПП1}}) \cdot (1 - P_{\text{ПП2}}) \cdot P_{\text{ПП3}} + \mathbf{L} + (1 - P_{\text{ПП1}}) \cdot \mathbf{L} \cdot (1 - P_{\text{ППN-1}}) \cdot P_{\text{ППN}}, \quad (7)$$

где $P_{\text{ПП}i}$ – вероятность подбора пароля при наборе i-й комбинации с учетом того, что $i - 1$ комбинаций уже опробовано и нет смысла набирать их заново;

$$P_{\text{ПП}i} = \frac{1}{N - i + 1},\ i = 1,2,...,N.$$

Подставив в формулу (7) выражения для $P_{\text{ПП}i}$, получим

$$P_{\text{ПП}} = \frac{1}{N} + (1 - \frac{1}{N}) \cdot \frac{1}{N-1} + (1 - \frac{1}{N}) \cdot (1 - \frac{1}{N-1}) \cdot \frac{1}{N-2} + \mathbf{L} + (1 - \frac{1}{N}) \cdot \mathbf{L} \cdot (1 - \frac{1}{N-N+2}) \cdot \frac{1}{N-N+1} =$$

$$= \frac{1}{N} + \frac{N-1}{N} \cdot \frac{1}{N-1} + \frac{N-1}{N} \cdot \frac{N-2}{N-1} \cdot \frac{1}{N-2} + \mathbf{L} + \frac{N-1}{N} \cdot \mathbf{L} \cdot \frac{N-N+1}{N-N+2} \cdot \frac{1}{N-N+1} =$$

$$= \frac{1}{N} + \frac{1}{N} + \frac{1}{N} + \mathbf{L} + \frac{1}{N} = N \cdot \frac{1}{N} = 1.$$

При использовании принципа ограничения попыток вероятность подбора пароля за k попыток будет равна

$$P_{\text{ПП}} = \frac{1}{N} + (1 - \frac{1}{N}) \cdot \frac{1}{N-1} + \mathbf{L} + (1 - \frac{1}{N}) \cdot \mathbf{L} \cdot (1 - \frac{1}{N-k+2}) \cdot \frac{1}{N-k+1} = \frac{k}{N}, \quad (8)$$

где k – допустимое количество попыток неправильного входа в систему.

Вероятность подбора пароля за k попыток означает, что пароль будет подобран с первой попытки или будет подобран со второй попытки или… и так далее …будет подобран с k-й попытки.

Поэтому в формулах (7) и (8) каждое слагаемое является вероятностью подбора пароля с определенной попытки.

Таким образом, вероятность подбора пароля с i-й попытки определяется по следующей формуле:

$$P_{\text{СП}} = (1 - P_{\text{ПП1}}) \cdot (1 - P_{\text{ПП2}}) \cdot \mathbf{L} \cdot (1 - P_{\text{ПП}i-1}) P_{\text{ПП}i}, \quad (9)$$

где $P_{\text{СП}}$ – вероятность подбора пароля с i-й попытки.

Подставив в формулу (8) выражения для $P_{ППi}$, получим

$$P_{СП} = (1-\frac{1}{N})\cdot(1-\frac{1}{N-1})\cdot \mathbf{L} \cdot (1-\frac{1}{N-i+2})\cdot\frac{1}{N-i+1} = \frac{1}{N}. \qquad (10)$$

Реализация данного принципа заключается в блокировке средства аутентификации при превышении допустимого количества попыток неправильного входа в систему.

Принцип цикличности заключается в том, что средство опознания функционирует по заранее установленному жесткому циклу, и ни при каких входных воздействиях цикл его работы не нарушается.

При использовании данного принципа в качестве параметра, учет которого позволяет повысить эффективность средства опознания, выступает безопасное время действия пароля, связанное с вероятностью его подбора простым соотношением:

$$T_{без} = \frac{P_Т}{P_1}T_ц = N \cdot P_Т \cdot T_ц, \qquad (11)$$

где $T_{без}$ – безопасное время действия пароля;

$P_Т$ – вероятность подбора пароля за время $T_{без}$;

$T_ц$ – время выполнения средством опознания одного цикла работы.

В силу того что цикл работы жестко фиксирован, путем ввода некоторой временной задержки в конце цикла можно существенно повысить безопасное время пароля при постоянной вероятности подбора пароля. В данном случае безопасное время действия пароля определяется так:

$$T_{без} = \frac{P_Т}{P_1}\cdot(T_ц + t_з) = N \cdot P_Т \cdot (T_ц + t_з), \qquad (12)$$

где $t_з$ – временная задержка.

Отсюда

$$P_Т = \frac{T_{без}}{N\cdot(T_ц + t_з)}. \qquad (13)$$

Так как безопасное время действия пароля принято измерять, как минимум, в часах, а время выполнения средством опознания одного цикла работы и временной задержки – в секундах, то в формулу (13) следует ввести коэффициент, переводящий безопасное время действия пароля в часы:

$$P_Т = \frac{3600\cdot T_{без}}{N\cdot(T_ц + t_з)}. \qquad (14)$$

В этом случае вероятность подбора пароля за безопасное время его действия определяется по формуле:

$$P_{\text{Т}} = \frac{3600 \cdot T_{\text{без}}}{A^n \cdot (T_{\text{ц}} + t_{\text{з}})}. \quad (15)$$

При использовании PIN-кода формула (16) имеет следующий вид:

$$P_{\text{Т}} = \frac{3600 \cdot T_{\text{без}}}{10^n \cdot (T_{\text{ц}} + t_{\text{з}})}. \quad (16)$$

При использовании двоичного ключа формула (14) имеет следующий вид:

$$P_{\text{Т}} = \frac{3600 \cdot T_{\text{без}}}{2^n \cdot (T_{\text{ц}} + t_{\text{з}})}. \quad (17)$$

Во многих средствах опознания предусматривается возможность субъектам самим назначать себе пароли независимо друг от друга. В этом случае существует вероятность того, что у двух разных пользователей могут оказаться одинаковые пароли. Это приводит к тому, что средство опознания при обращении к ней одного субъекта может принять его за другого. Поэтому такие системы опознания должны проверяться по критерию «парадокс дней рождения».

Математически парадокс дней рождений формируется следующим образом. Если $an^{-0,5}$ предметов выбирается с возвращением из некоторой совокупности размером n, то вероятность того, что два из них окажутся одинаковыми, составляет величину

$$P_{\text{Д}} = 1 - e^{(-\frac{a^2}{2})}. \quad (18)$$

Практически это означает, что в случайно подобранной группе из 24 человек вероятность наличия двух лиц с одним и тем же днём рождения составляет величину порядка 0,5.

Если количество пользователей системы принять за d, то тогда

$$a = \frac{d}{A^{n/2}}. \quad (19)$$

Подставив выражение (19) в выражение (18), получим

$$P_{\text{Д}} = 1 - e^{(-\frac{d^2}{2 \cdot A^n})}. \quad (20)$$

3. Порядок выполнения работы

1. Изучить краткие сведения из теории.

2. Изучить методику выбора оптимальных параметров парольной системы. Используя доступные прикладные программы персональных компьютеров (ПК), определить минимально необходимую длину пароля для семи алфавитов,

удовлетворяющую следующим условиям: вероятность подбора пароля с первой попытки $P_1 = 10^{-13}$; вероятность подбора пароля за время $T_{без} = 10$ ч $P_Т = 10^{-7}$; время одной попытки подбора пароля $t = 60$ с; вероятность появления двух одинаковых паролей при общем количестве субъектов $n = 10\,000$ $P_Д = 10^{-6}$.

Алфавиты:

– $A_1 = 10$ (цифры);
– $A_2 = 26$ (английский);
– $A_3 = 33$ (русский);
– $A_4 = 36$ (цифры+английский);
– $A_5 = 43$ (цифры+русский);
– $A_6 = 59$ (английский+русский);
– $A_7 = 69$ (цифры+английский+русский).

Результаты расчетов занести в табл. 1.1. Вывод расчетных формул и ход решения поместить в отчет.

Таблица 1.1

	$k(P_1)$	$k(P_T)$	$k(P_Д)$
A_1			
A_2			
A_3			
A_4			
A_5			
A_6			
A_7			

3. Оценить вероятности подбора пароля с n-й и за n попыток. Используя доступные прикладные программы ПК, определить вероятности подбора пароля с первой попытки, с десятой попытки и за десять попыток для семи алфавитов при длине пароля $k = 4$.

Алфавиты:

– $A_1 = 10$ (цифры);
– $A_2 = 26$ (английский);
– $A_3 = 33$ (русский);
– $A_4 = 36$ (цифры+английский);
– $A_5 = 43$ (цифры+русский);
– $A_6 = 59$ (английский+русский);
– $A_7 = 69$ (цифры+английский+русский).

Результаты расчетов занести в табл. 1.2. Вывод расчетных формул и ход решения поместить в отчет.

Таблица 1.2

	P_1	P_{c10}	$P_{за10}$
A_1			
A_2			
A_3			
A_4			
A_5			
A_6			
A_7			

4. Используя доступные прикладные программы ПК, определить вероятности подбора пароля с первой попытки для семи алфавитов при длине пароля $k = 5$ для следующих случаев:

a) символы в пароле могут повторяться;

b) символы в пароле не повторяются.

Алфавиты:

- $A_1 = 10$ (цифры);
- $A_2 = 26$ (английский);
- $A_3 = 33$ (русский);
- $A_4 = 36$ (цифры+английский);
- $A_5 = 43$ (цифры+русский);
- $A_6 = 59$ (английский+русский);
- $A_7 = 69$ (цифры+английский+русский).

Результаты расчетов занести в табл. 1.3. Вывод расчетных формул и ход решения поместить в отчет.

Таблица 1.3

	P_1	$P_{1неповт}$
A_1		
A_2		
A_3		
A_4		
A_5		
A_6		
A_7		

5. Используя доступные прикладные программы ПК, определить вероятности подбора комбинированного пароля с первой попытки и за время $T = 2$ ч, ес-

ли первая часть пароля является 16-байтной произвольной строкой из некоторого файла, а вторая часть пароля задается для семи алфавитов при длине ключа $k_2 = 4$ символа. Время ввода одного варианта каждой части комбинированного пароля $t = 10$ с.

Алфавиты:

– $A_1 = 10$ (цифры);

– $A_2 = 26$ (английский);

– $A_3 = 33$ (русский);

– $A_4 = 36$ (цифры+английский);

– $A_5 = 43$ (цифры+русский);

– $A_6 = 59$ (английский+русский);

– $A_7 = 69$ (цифры+английский+русский).

Результаты расчетов занести в табл. 1.4. Вывод расчетных формул и ход решения поместить в отчет.

Таблица 1.4

	P_1	P_T
A_1		
A_2		
A_3		
A_4		
A_5		
A_6		
A_7		

6. Оценить время, необходимое для подбора пароля. Используя доступные прикладные программы ПК, определить время подбора пароля для следующих случаев:

а) алфавит A = 69, длина пароля $k = 4$, время ввода одного символа пароля $t' = 0{,}5$ с;

б) алфавит A = 59, длина пароля $k = 4$, время ввода одного символа пароля $t' = 0{,}5$ с, после каждого набора пароля клавиатура блокируется на $t_б = 3$ с;

в) алфавит A = 43, длина пароля $k = 4$, время ввода одного символа пароля $t' = 0{,}5$ с, после каждого десятого набора пароля клавиатура блокируется на $t_б = 5$ с;

г) алфавит A = 10, длина пароля $k = 4$, время ввода одного символа пароля $t' = 0{,}5$ с, после первого набора пароля клавиатура блокируется на $t_б = 1$ с, после второго – на $t_б = 2$ с, после i-го – на $t_б = i$ с.

Вывод расчетных формул и ход решения поместить в отчет.

7. Произвести оценку необходимой длины пароля для удовлетворения требований, предъявляемых к системе опознания. Используя доступные прикладные программы ПК, определить минимальную достаточную длину пароля, удовлетворяющую следующим параметрам: алфавит A = 69, время ввода одного символа пароля t' = 0,5 с, вероятность подбора пароля за время, отводимое на подбор пароля, $T_{без}$ = 92 дня, $P_T = 10^{-5}$.

Вывод расчетных формул и ход решения поместить в отчет.

8. По заданию преподавателя, используя доступные прикладные программы ПК, решить шесть дополнительных задач (из списка задач для самостоятельного решения). Вывод расчетных формул и ход решения для каждой задачи отразить в отчете.

4. Примеры решения задач

Задача 1. Определить, каким должно быть минимальное число символов в пароле для удовлетворения следующим условиям: вероятность определения пароля с первого раза $P_1 = 10^{-10}$; алфавит $A = 10$.

Решение.

Вероятность подбора пароля с первой попытки определяется следующим выражением:

$$P_1 = \frac{1}{A^k}.$$

Выразим k:

$$A^k = \frac{1}{P_1}; \; k = \log_A \frac{1}{P_1}.$$

Подставив исходные данные, получим

$$k = \log_{10} 10^{10} = 10.$$

Ответ: $k = 10$.

Задача 2. Определить вероятность подбора пароля за 8 ч (T) при длине ключа $k = 4$, алфавите $A = 30$ и времени ввода одного символа $t = 1$ с.

Решение.

Вероятность подбора пароля за безопасное время его действия определяется по следующей формуле:

$$P_{\text{Т}} = \frac{3600 \cdot T_{\text{без}}}{A^n \cdot (T_{\text{ц}} + t_{\text{з}})}.$$

Подставив исходные данные, получим

$$P_{\text{Т}} = \frac{3600 \cdot T}{A^k \cdot k \cdot t} = \frac{3600 \cdot 8}{30^4 \cdot 4 \cdot 1} = \frac{7200}{81} \cdot 10^{-4} = 8{,}89 \cdot 10^{-3}.$$

Ответ: $P_{\text{Т}} = 8{,}89 \cdot 10^{-3}$.

Задача 3. Определить вероятность подбора пароля за три попытки при длине ключа k=4 и алфавите A=20.

Решение.

Вероятность подбора пароля за три попытки определяется выражением

$$P_{\text{ПП}} = \frac{3}{N}.$$

Объем алфавита для паролей определяется следующим выражением:

$$N = A^k.$$

Тогда

$$P_{\text{ПП}} = \frac{3}{20^4} = 3 \cdot 20^{-4} = 1{,}875 \cdot 10^{-5}.$$

Ответ: $P_{\text{ПП}} = 1{,}875 \cdot 10^{-5}$.

Задача 4. Определить вероятность подбора комбинированного пароля за 8 ч (T), состоящего из двух частей: длиной $k_1 = 8$ из алфавита $A_1 = 10$ и длиной $k_2 = 4$ из алфавита $A_2 = 20$ при времени ввода первой части ключа $t_1 = 2$ с, а второй $t_2 = 1$ с.

Решение.

Вероятность подбора комбинированного пароля определяется по следующей формуле:

$$P_{\text{Т}} = P_{\text{Т}1} \cdot P_{\text{Т}2}.$$

Вероятность подбора пароля за безопасное время его действия определяется по следующей формуле:

$$P_{\text{Т}} = \frac{3600 \cdot T_{\text{без}}}{A^n \cdot (T_{\text{ц}} + t_{\text{з}})}.$$

Тогда

$$P_{\text{Т}} = \frac{3600 \cdot 8}{10^8 \cdot 2} \cdot \frac{3600 \cdot 8}{20^4 \cdot 1} = 14\,400 \cdot 10^{-8} \cdot 1800 \cdot 10^{-4} = 2{,}592 \cdot 10^{-5}.$$

Ответ: $P_{\text{Т}} = 2{,}592 \cdot 10^{-5}$.

Задача 5. Определить минимальную длину ключа необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время T = 4000 ч $P_{\text{Т}} = 10^{-10}$; алфавит A = 10; время набора одного символа t = 2 с.

Решение.

Вероятность подбора пароля за безопасное время его действия определяется по следующей формуле:

$$P_{\text{Т}} = \frac{3600 \cdot T_{\text{без}}}{A^n \cdot (T_{\text{ц}} + t_{\text{з}})}.$$

Время выполнения средством опознания одного цикла работы в таком случае будет вычисляться следующим образом:

$$T_{\text{ц}} = k \cdot t.$$

Тогда

$$P_{\text{Т}} = \frac{3600 \cdot T_{\text{без}}}{A^n \cdot (k \cdot t + t_{\text{з}})}.$$

Отсюда, при условии, что $t_{\text{з}} = 0$, получим

$$k \cdot A^k \geq \frac{3600 \cdot T}{P_{\text{Т}} \cdot t}.$$

Подставив исходные данные, получим

$$k \cdot 10^k \geq \frac{3600 \cdot 4000}{10^{-10} \cdot 2}; k \cdot 10^k \geq 7{,}2 \cdot 10^{16}; k = 16.$$

Ответ: $k = 16$.

Задача 6. Определить время подбора пароля, состоящего из шести символов (k) из алфавита $A = 20$ при времени ввода одного символа $t = 3$ с.

Решение.

Вероятность подбора пароля за безопасное время его действия определяется по следующей формуле:

$$P_{\text{Т}} = \frac{3600 \cdot T_{\text{без}}}{A^n \cdot (T_{\text{ц}} + t_{\text{з}})}.$$

Отсюда, при условии, что $P_{\text{Т}} = 1$, $T_{\text{ц}} = k \cdot t$ и $t_{\text{з}} = 0$, получим

$$T = \frac{A^k \cdot t \cdot k}{3600}.$$

Подставив исходные данные, получим

$$T = \frac{20^6 \cdot 3 \cdot 6}{3600} = 36{,}5 \text{ года}.$$

Ответ: $T = 36{,}5$ года.

5. Задачи для самостоятельного решения

1.1. Определить, каким должно быть минимальное число символов в пароле для удовлетворения следующим условиям: вероятность подбора пароля с первой попытки $P_1 = 10^{-10}$; алфавит $A = 10$.

1.2. Определить, каким должно быть минимальное число символов в пароле для удовлетворения следующим условиям: вероятность подбора пароля с первой попытки $P_1 = 10^{-12}$; алфавит $A = 10$.

1.3. Определить, каким должно быть минимальное число символов в пароле для удовлетворения следующим условиям: вероятность подбора пароля с первой попытки $P_1 = 10^{-15}$; алфавит $A = 10$.

1.4. Определить, каким должно быть минимальное число символов в пароле для удовлетворения следующим условиям: вероятность подбора пароля с первой попытки $P_1 = 10^{-8}$; алфавит $A = 100$.

1.5. Определить, каким должно быть минимальное число символов в пароле для удовлетворения следующим условиям: вероятность подбора пароля с первой попытки $P_1 = 10^{-12}$; алфавит $A = 100$.

1.6. Определить, каким должно быть минимальное число символов в пароле для удовлетворения следующим условиям: вероятность подбора пароля с первой попытки $P_1 = 10^{-15}$; алфавит $A = 1000$.

2.1. Определить вероятность подбора пароля с первой попытки при длине ключа $k = 4$ и алфавите $A = 10$.

2.2. Определить вероятность подбора пароля с первой попытки при длине ключа $k = 4$ и алфавите $A = 20$.

2.3. Определить вероятность подбора пароля за 8 ч (T) при длине ключа $k = 4$, алфавите $A = 10$ и времени ввода одного символа $t = 1$ с.

2.4. Определить вероятность подбора пароля за 8 ч (T) при длине ключа $k = 4$, алфавите $A = 30$ и времени ввода одного символа $t = 1$ с.

2.5. Определить вероятность подбора пароля за 16 ч (T) при длине ключа $k = 4$, алфавите $A = 50$ и времени ввода одного символа $t = 1$ с.

2.6. Определить вероятность подбора пароля за 4 ч (T) при длине ключа $k = 7$, алфавите $A = 60$ и времени ввода одного символа $t = 1$ с.

3.1. Определить вероятность подбора пароля с десятого раза при длине ключа $k = 4$ и алфавите $A = 10$.

3.2. Определить вероятность подбора пароля с десятого раза при длине ключа $k = 4$ и алфавите $A = 20$.

3.3. Определить вероятность подбора пароля за три набора при длине ключа $k = 4$ и алфавите $A = 10$.

3.4. Определить вероятность подбора пароля за три набора при длине ключа $k = 4$ и алфавите $A = 20$.

3.5. Определить вероятность подбора пароля за десять наборов при длине ключа $k = 4$ и алфавите $A = 10$.

3.6. Определить вероятность подбора пароля за десять наборов при длине ключа $k = 4$ и алфавите $A = 20$.

4.1. Определить вероятность подбора комбинированного пароля с первой попытки, состоящего из двух частей: длины $k_1 = 4$, алфавита $A_1 = 10$ и длины $k_2 = 8$, алфавита $A_2 = 20$.

4.2. Определить вероятность подбора комбинированного пароля с первой попытки, состоящего из двух частей: длины $k_1 = 8$, алфавита $A_1 = 10$ и длины $k_2 = 4$, алфавита $A_2 = 20$.

4.3. Определить вероятность подбора комбинированного пароля за 8 ч (T), состоящего из двух частей: длины $k_1 = 8$, алфавита $A_1 = 10$ и длины $k_2 = 4$, алфавита $A_2 = 20$ при времени ввода первой части ключа $t_1 = 2$ с, а второй $t_2 = 1$ с.

4.4. Определить вероятность подбора комбинированного пароля за 8 ч (T), состоящего из двух частей: длины $k_1 = 5$, алфавита $A_1 = 10$ и длины $k_2 = 8$, алфавита $A_2 = 20$ при времени ввода первой части ключа $t_1 = 1$ с, а второй $t_2 = 2$ с.

4.5. Определить вероятность подбора комбинированного пароля за 8 ч (T), состоящего из двух частей: длины $k_1 = 6$, алфавита $A_1 = 10$ и длины $k_2 = 8$, алфавита $A_2 = 20$ при времени ввода первой части ключа $t_1 = 1$ с, а второй $t_2 = 4$ с.

4.6. Определить вероятность подбора комбинированного пароля за 10 ч (T), состоящего из двух частей: длины $k_1 = 6$, алфавита $A_1 = 10$ и длины $k_2 = 5$, алфавита $A_2 = 20$ при времени ввода первой части ключа $t_1 = 2$ с, а второй $t_2 = 3$ с.

5.1. Определить минимальную длину ключа, необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время T = 4000 ч $P_T = 10^{-10}$; алфавит A = 10; время набора одного символа t = 2 с.

5.2. Определить минимальную длину ключа, необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время T = 400 ч $P_T = 10^{-6}$; алфавит A = 10; время набора одного символа t = 4 с.

5.3. Определить минимальную длину ключа, необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время T = 4 ч $P_T = 10^{-10}$; алфавит A = 10; время набора одного символа t = 10 с.

5.4. Определить минимальную длину ключа, необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время T = 100 ч $P_T = 10^{-6}$; алфавит A = 20; время набора одного символа t = 3 с.

5.5. Определить минимальную длину ключа, необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время T = 1000 ч $P_T = 10^{-5}$; алфавит A = 20; время набора одного символа t = 1 с.

5.6. Определить минимальную длину ключа, необходимую для удовлетворения парольной системой следующих условий: вероятность подбора пароля за время T = 100 ч $P_T = 10^{-10}$; алфавит A = 20; время набора одного символа t = 2 с.

6.1. Определить время подбора пароля, состоящего из семи символов (k), из алфавита A = 10 при времени ввода одного символа t = 2 с.

6.2. Определить время подбора пароля, состоящего из пяти символов (k), из алфавита A = 10 при времени ввода одного символа t = 1 с.

6.3. Определить время подбора пароля, состоящего из шести символов (k), из алфавита A = 10 при времени ввода одного символа t = 5 с.

6.4. Определить время подбора пароля, состоящего из шести символов (k), из алфавита A = 20 при времени ввода одного символа t = 3 с.

6.5. Определить время подбора пароля, состоящего из трех символов (k), из алфавита A = 20 при времени ввода одного символа t = 1 с.

6.6. Определить время подбора пароля, состоящего из четырех символов (k), из алфавита A = 20 при времени ввода одного символа t = 3 с.

6. Содержание отчета:

1. Краткие сведения из теории.
2. Условие задачи.
3. Вывод расчетных формул.
4. Результаты расчетов.
5. Выводы.

ЛИТЕРАТУРА

1. Зима, В. М. Защита компьютерных ресурсов от несанкционированных действий пользователя : учебное пособие / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – СПб. : Издательство ВИКА им. А.Ф. Можайского, 1997. – 362 с.

2. Зегжда, Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М. : Горячая линия – Телеком, 2000. – 452 с.

3. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М. : Радио и связь, 2001. – 376 с.

4. Белкин, П. Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных : учеб. пособие для вузов / П. Ю. Белкин. – М. : Радио и связь, 2000. – 168 с.

5. Дшхуннян, В. Л. Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты / В. Л. Дшхуннян. – М. : ООО «Издательство АСТ», Издательство «НТ Пресс», 2004. – 695 с.

Св. план 2008, поз. 97

Учебное издание

ПАРОЛЬНЫЕ МЕТОДЫ ОПОЗНАНИЯ В СЕТЯХ ТЕЛЕКОММУНИКАЦИЙ

Методические указания
к лабораторной работе

по дисциплине «Защита программного обеспечения
и баз данных в сетях телекоммуникаций»
для студентов специальностей I-45 01 03 «Сети телекоммуникаций»
и I-98 01 02 «Защита информации в телекоммуникациях»
всех форм обучения

Составители:
Бобов Михаил Никитич
Буй Павел Михайлович

Редактор Т. П. Андрейченко
Корректор М. В. Тезина

Подписано в печать 22.07.2008. Формат 60×84 1/16. Бумага офсетная.
Гарнитура «Таймс». Печать ризографическая. Усл. печ. л. 1,74.
Уч.-изд. л. 1,5. Тираж 75 экз. Заказ 191.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0056964 от 01.04.2004. ЛП №02330/0131666 от 30.04.2004.
220013, Минск, П. Бровки, 6