Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Система широковещательной передачи анонимных сообщений

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Вдошкина Никиты Владимировича

Научный руководитель

доцент, к.ф.-м.н. _____ А.В. Жаркова

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

В настоящее время обеспечение анонимности пользователей в сети Интернет становится всё более обсуждаемой и актуальной темой. Повышенное внимание общества к цензуре и методам борьбы с ней, постоянный рост количества преступлений в информационной сфере, забота государства о частной жизни и персональных данных граждан, – данные тезисы всё чаще появляются в средствах массовой информации и являются предметом постоянных дискуссий в правительстве и обществе.

Проблема обеспечения математически доказуемой абсолютной анонимности субъекта при взаимодействии его с адресатом в информационной системе сейчас не решена и относится к ряду концептуальных проблем современных информационных технологий. Теоретической основой для создания систем с возможностью отправки анонимных сообщений является проблема обедающих криптографов.

Целью данной дипломной работы является создание системы широковещательной передачи анонимных сообщений.

Для достижения поставленной цели требуется решить следующие задачи:

- изучить проблему обедающих криптографов;

- рассмотреть различные алгоритмы и протоколы, необходимые для реализации системы.

Дипломная работа состоит из введения, 6 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 80 страниц, из них 50 страниц – основное содержание, включая 17 рисунков, список использованных источников из 16 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Во введении ставятся цели и задачи дипломной работы.

В первом разделе «Необходимые определения» дипломной работы приводятся необходимые определения, используемые в работе.

Во втором разделе «Проблема обедающих криптографов» рассматривается проблема обедающих криптографов.

В статье [8] Дэвид Чаум вводит так называемую проблему обедающих криптографов: «Три криптографа собрались за обеденным столом. Официант сообщает им, что их еда уже была кем-то оплачена. Это может быть один из криптографов или АНБ. Криптографы уважают право друг друга совершить оплату анонимно, но хотят выяснить, заплатило ли АНБ».

Для решения данной проблемы Чаум предлагает следующее решение. Каждый криптограф подбрасывает монетку между собой и коллегой справа, закрывая меню так, чтобы только они двое видели результат. Затем каждый криптограф громко объявляет, как упали две монеты – одна его, и одна соседа слева: «одинаково» или «по-разному». Если один из криптографов произвел оплату, он утверждает противоположное тому, что видит. Если число возгласов «по-разному» будет нечетным, это означает, что обед оплатил криптограф; если четным – АНБ (при условии, что обед можно оплатить только один раз). Однако, если обед оплачивал криптограф, из сделанных заявлений никто из двух других не узнает, кто же конкретно оплатил счет.

Таким образом, данная схема позволяет анонимно опубликовывать 1 бит информации за 1 раунд. В дальнейшем данную схему будем называть базовым протоколом.

Для публикации всего сообщения при помощи данной схемы необходимо повторять базовый протокол снова и снова, пока сообщение не будет полностью опубликовано, т.е. отправитель просто начинает инвертировать свои высказывания в раундах, соответствующих единице в двоичном представлении сообщения. Если отправитель понимает, что его сообщение «перемешивается» с

каким-то другим сообщением, то он должен подождать случайным образом выбранное число раундов и попробовать передать сообщение заново.

Для обобщения протокола на любое количество участников каждый пользователь должен иметь общий секретный бит с каждым из участников. Каждый пользователь отправляет сумму по модулю 2 всех секретных битов, которые он разделяет. Если отправитель хочет опубликовать 1, то ему необходимо инвертировать сумму всех секретных битов по модулю 2 и отправить ее, если же отправитель хочет опубликовать 0 – отправить сумму всех секретных битов по модулю 2 без изменений. Если никто из участников не инвертировал свой результат, то сумма всех отправленных результатов должна равняться 0 по модулю 2, т.к. каждый секретный бит входит в результат дважды, иначе – сумма будет равна 1 по модулю 2. Для n раундов потребуется разделять n-битный секретный ключ с каждым из участников беседы, т.к. i-й бит секретного ключа используется только в i-м раунде. При обнаружении коллизии необходимо повторно осуществить действия, необходимые для отправки 1 бита.

Не обнаружение коллизии возможно только при одновременной передаче нечетным количеством отправителей идентичных участков сообщений.

В третьем разделе «Аутентификация» рассматриваются основы аутентификации. Установление (то есть проверка и подтверждение) подлинности всех аспектов информационного взаимодействия является важной составной частью проблемы обеспечения достоверности получаемой информации. Особенно остро эта проблема стоит в случае не доверяющих друг другу сторон, когда источником угроз может служить не только третья сторона (противник), но и сторона, с которой осуществляется взаимодействие. Рассмотрим основные положения протоколов аутентификации.

Во всех протоколах аутентификации присутствуют два участника:

1) A – доказывающий – участник, проходящий аутентификацию;

2) B – проверяющий – участник, проверяющий аутентичность A.

Целью протокола является проверка того, что участник A является тем, за

кого себя выдает.

С точки зрения B возможны два варианта возможного исхода протокола аутентификации: подтверждение личности A или отсутствие такого подтверждения.

1) Можно провести классификацию протоколов аутентификации по тому, на чем основана аутентификация:

1) протоколы, основанные на информации, которая известна обоим участникам. Такой информацией могут стать секреты, открытые ключи, пароли;

2) протоколы, использующие приборы, с помощью которых и проводится аутентификация. Такими приборами могут являться, например, магнитные или интеллектуальные пластиковые карты;

3) протоколы, использующие физические параметры участника A. В качестве таких параметров могут выступать, например, отпечатки пальцев, подписи, характеристики голоса.

Одной из основных целей аутентификации является обеспечение контроля доступа к определенным ресурсам, таким, как базы данных, здания, компьютерные программы, телекоммуникационные каналы связи, банковские счета.

В четвертом разделе «Криптографические хэш-функции» рассказывается о хэш-функциях, приводятся описания стандартов SHA и ГОСТ Р 34.11-2012.

Хэш-функции применяются при проведении статистических экспериментов, при тестировании логических устройств, при построении алгоритмов быстрого поиска и проверки целостности данных. Например, для реализации быстрого поиска требуемого сообщения в большом списке сообщений разной длины удобнее всего сравнивать друг с другом не сами сообщения, а короткие значения их сверток, играющих роль контрольных сумм. Основным требованием, предъявляемым к таким хэш-функциям, является равномерность распределения их значений для случайно выбранных значений аргументов.

В криптографических целях хэш-функции используются для решения следующих задач:

1) построение системы контроля целостности данных при их передаче или хранении;

2) аутентификация источника данных.

Для решения первой задачи для каждого набора данных вычисляется значение хэш-функции (называемое *кодом аутентификации* сообщения или *имитовставкой*), которое передается или хранится вместе с самими данными. При получении данных пользователь вычисляет значение хэш-функции и сравнивает его с имеющимся контрольным значением. Несовпадение значений может свидетельствовать о том, что данные были изменены.

Хэш-функция, которая используется при этом, должна иметь возможность (в отличие от обычной контрольной суммы) осуществлять обнаружение не только случайных ошибок в наборах данных, возникающих при их хранении и передаче, но и сигнализировать об активных атаках противника, пытающегося осуществить навязывание ложной информации. Для того чтобы нарушитель не смог самостоятельно вычислить контрольное значение хэш-функции и тем самым осуществить успешную имитацию или подмену данных, хэш-функция должна зависеть от ключа пользователя, который не известен злоумышленнику. Только передающая и принимающая стороны должны знать этот ключ. Такой тип хэш-функции будем называть *ключевыми*.

В пятом разделе «Генератор псевдослучайных последовательностей» рассматриваются основы генераторов псевдослучайных чисел и проводятся алгоритмов генерации Блюма-Микали и Блюма-Блюма-Шуба.

В литературе последовательности, сгенерированные арифметическим способом, называются *псевдослучайными*, а метод их генерации называют *генератором псевдослучайных последовательностей*.

Псевдослучайные последовательности используются давно и повсеместно. Перечислим некоторые области их применения:

1) социологические и научные исследования. Подготовка псевдослучайных выборок при сборе данных, опросе мнений или в исследовании физических явлений с псевдослучайным выбором результатов экспериментов;

2) моделирование. В компьютерном моделировании физических явлений. Кроме того, математическое моделирование использует псевдослучайные последовательности как один из инструментов численного анализа;

3) криптография и информационная безопасность. Псевдослучайные последовательности могут использоваться в тестировании корректности или эффективности алгоритмов и программ. Многие алгоритмы используют генерацию псевдослучайных последовательностей для решения прикладных задач (например, криптографические алгоритмы шифрования, генерация уникальных идентификаторов и др.);

4) принятие решений в автоматизированных экспертных системах. Использование псевдослучайных последовательностей является частью стратегий принятия решений. Например, для беспристрастности выбора экзаменационного билета студентом на экзамене. Псевдослучайные генераторы также используются в теории матричных игр;

5) оптимизация функциональных зависимостей. Некоторые математические методы оптимизации используют стохастические методы для поиска экстремумов функций;

6) развлечения и игры. Псевдослучайность в играх играет значительную роль. В компьютерных или настольных играх случайность помогает разнообразить игровой процесс.

В шестом разделе «Программная реализация» описывается созданная система широковещательной передачи анонимных сообщений. В ходе проделанной работы была разработана и реализована программа для обмена анонимными широковещательными сообщениями, в том числе с использованием отечественной функции хэширования ГОСТ Р 34.11-2012 и алгоритма генерации псевдослучайных последовательностей Блюма-Блюма-

Шуба, основанная на проблеме обедающих криптографов. Данная программа представлена двумя модулями: клиентская и серверная часть.

Программа была написана на языке Java с помощью компилятора Intellij IDEA (листинг клиентской программы представлен в приложении А, серверной – в приложении Б).

Для передачи широковещательных анонимных сообщений текст разбивается на символы. Для двоичного представления символов берется их 16-битный ASCII код. Опишем алгоритм, реализованный в программе.

1) Клиент подсчитывает длину двоичного представления сообщения, которое он хочет отправить и отправляет серверу полученное значение.

2) В ответ сервер присылает номером раунда, в котором клиент должен начать передачу сообщения.

3) В каждом раунде пользователь отправляет серверу бит, равный сумме по модулю 2 разделяемых раундовых ключей с подключенными пользователями по модулю 2; если в данном раунде клиент передает сообщение, то к этой сумме по модулю 2 добавляет соответствующее значение бита сообщения.

4) Сервер подсчитывает сумму по модулю 2 всех бит, полученных от всех подключенных пользователей в течение раунда.

5) Если номер раунда кратен 16, то сервер подсчитывает ASCII-код символа, который был получен за последние 16 раундов, и отправляет соответствующий символ всем подключенным пользователям.

ЗАКЛЮЧЕНИЕ

Проблема обеспечения математически доказуемой абсолютной анонимности субъекта при взаимодействии его с адресатом в информационной системе сейчас не решена и относится к ряду концептуальных проблем современных информационных технологий. Теоретической основой для создания систем с возможностью отправки анонимных сообщений является проблема обедающих криптографов.

В ходе данной дипломной работы была рассмотрена и переведена статья [8], изучены проблема обедающих криптографов, которая является теоретической основой для создания канала связи с возможностью передачи анонимных сообщений, функции хэширования SHA и ГОСТ Р 34.11-2012 и алгоритмы генерации псевдослучайных последовательностей Блюма-Микали и Блюма-Блюма-Шуба.

Описанные в данной работе решения проблемы обедающих криптографов демонстрируют возможность создания канала, в котором отследить отправителя сообщения, будет весьма затруднительно. Также показано, что в данной системе может быть использовано шифрование с открытым ключом для отправки личных сообщений конкретным пользователям данной сети. Описанный подход может быть использован для решения широкого спектра практических проблем.

В результате проделанной работы была разработана и реализована система, позволяющая обмениваться анонимными широковещательными сообщениями, в том числе с использованием отечественной функции хэширования ГОСТ Р 34.11-2012 и алгоритма генерации псевдослучайных последовательностей Блюма-Блюма-Шуба.

Таким образом, все поставленные задачи были полностью решены, цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Салий, В. Н. Криптографические методы и средства защиты информации : учеб. пособие [Электронный ресурс] / В. Н. Салий. Саратов : 2012. 41 с. Загл. с экрана. Яз. рус.

2 Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. 2-е изд., испр. и доп. М. : Гелиос АРВ, 2002. 480 с.

3 Богомолов, А. М. Алгебраические основы теории дискретных систем / А. М. Богомолов, В. Н. Салий. М. : Наука, 1997. 368 с.

4 Соловьева, Ф. И. Введение в теорию кодирования: учеб. пособие [Электронный ресурс] / Ф. И. Соловьева. Новосибирск : 2006. 127 с. Загл. с экрана. Яз. рус.

5 Адигеев, М. Г. Введение в криптографию : учеб. пособие [Электронный ресурс] / М. Г. Адигеев. Ростов-на-Дону : 2002. 35 с. Загл. с экрана. Яз. рус.

6 Сборник руководящих документов по защите информации от несанкционированного дотсупа [Электронный ресурс] // Московский государственный университет имени М. В. Ломоносова [Электронный ресурс]. URL: http://www.msu.ru/info/is/docs/6/rd.pdf (дата обращения: 18.12.2016). Загл с экрана. Яз. англ.

7 Грэхем, Р. Конкретная математика / Р. Грэхем, Д. Крут, О. Паташник. М. : Мир, 1998. 703 с.

8 Chaum, D. The dining cryptographers problem: unconditional sender and recipient untraceability [Электронный ресурс] / D. Chaum. J. Cryptology, 1988. P. 65–75. Загл. с экрана. Яз. англ.

9 Scholz, I. Dining Cryptographers – The Protocol [Электронный ресурс] // CCC Event Weblog [Электронный ресурс] : About the Congress and other CCC events. URL: https://events.ccc.de/congress/2007/Fahrplan/attachments/981_ccc-paper.pdf (дата обращения: 18.12.2016). Загл с экрана. Яз. англ.

10 Golle, P. Dining Cryptographers Revisited [Электронный ресурс] // GNU's Framework for Secure Peer-to-Peer Networking [Электронный ресурс].

URL: https://www.gnunet.org/sites/default/files/golle-eurocrypt2004.pdf (дата обращения: 18.12.2016). Загл с экрана. Яз. англ.

11 Harreveld, T. Dining Cryptographer Networks [Электронный ресурс] // Department of Information and Computing Sciences [Электронный ресурс]. URL: http://www.cs.uu.nl/docs/vakken/b3sec/Proj12/Dining.pdf (дата обращения: 18.12.2016). Загл с экрана. Яз. англ.

12 Шнайер, Б. Прикладная криптография / Б. Шнайер. М. : Издательство ТРИУМФ, 2002. 816 с.

13 Баричев, С. Г. Основы современной криптографии [Электронный ресурс] / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. М. : Горячая линия – Телеком, 2001. 152 с.

14 ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования [Электронный ресурс] // СПЕЦРЕМОНТ [Электронный ресурс] : URL: http://specremont.su/pdf/gost_34_11_2012.pdf (дата обращения: 08.12.2016). Загл. с экрана. Яз. рус.

15 Слеповичев, И. И. Генераторы псевдослучайных чисел : учеб. пособие [Электронный ресурс] / И. И. Слеповичев. Саратов : 2016. 118 с. Загл. с экрана. Яз. рус.

16 Blum, L. A Simple Unpredictable Pseudo-Random Number Generator [Электронный ресурс] / L. Blum, M. Blum, M. Shub. J. SIAM J. on Computing, 1986. P. 364–383. Загл. с экрана. Яз. англ.