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

УДК 004.772

Зинькевич
Вячеслав Николаевич

Методы и средства организации защищенной передачи файлов

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Ярмолик В.Н.
д.т.н., профессор

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

В современном обществе с развитием информационных технологий все больший вес приобретает информация и ее обработка, способы хранения и передачи. С тех пор, как компьютеры стали распространены и перестали быть привилегией научных центров, а информационные хранилища стали вмещать громадные объемы данных, большая часть информации стала храниться в цифровом виде на различного рода накопителях. Данный способ является более удобным, простым и дешевым в сравнении со старыми методами. Современные сетевые технологии позволяют получать доступ к ресурсам из различных точек мира так, как будто необходимая информация находится на локальной рабочей машине.

Зачастую, информация является конфиденциальной и ценной, вследствие чего она должна быть защищена не только от возможности несанкционированного изменения и удаления, но и от посторонних глаз. Так как работа с документами и хранение их происходит на разных рабочих машинах, а передача осуществляется посредством сети, чаще всего открытой, то наиболее уязвимым местом является именно процесс передачи информации с рабочей машины клиента на сервер хранения. Для достижения этих безопасности передачи и хранения данных используется различные методы криптографии.

Существуют различные способы преобразования открытых данных в зашифрованные, основанные на симметричных и асимметричных алгоритмах. Симметричные криптосистемы используют один ключа для шифрования и дешифрования данных. Асимметричные в свою очередь опираются на пару ключей, называемых открытым и закрытым ключом.

В настоящее время для сокрытия информации используют различные способы защиты:

- контроль доступа к секретной информации;
- разграничение доступа;
- дублирование каналов связи и подключение резервных устройств;
- криптографические преобразования информации.

Так как передача данных часто происходит по открытым каналам данных, существуют определенные угрозы в нарушении целостности и конфиденциальности информации. Злоумышленник может осуществить перехват данных с целью их несанкционированное использование, модификацию передаваемой информации с целью порчи или введения в заблуждение получателя. В связи с этим необходимость защиты каналов связи стоит особенно остро в реализации передачи данных.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является анализ и разработка методов передачи файлов по защищенным каналам связи.

Для решения поставленной цели необходимо решить следующие основные задачи:

1. Проанализировать требования к протоколам передачи данных.
2. Рассмотреть существующие методы осуществления безопасной передачи файлов.
3. Проанализировать составные части, необходимые для разработки безопасной передачи: шифрование, аутентификация.
4. Проанализировать математический аппарат, позволяющий реализовать шифрование, распределение ключей и проверку авторства сообщений.
5. Предложить методы и средства обеспечения безопасной передачи.
6. Показать работоспособность представленного протокола передачи, разработав программный модуль.
7. Экспериментальным путем проверить работоспособность разработанного протокола, а также исследовать его влияние на скорость передачи.

Областью исследования в данной работе являются сетевые протоколы передачи данных.

Объектом исследования является протокол безопасной передачи данных транспортного уровня.

Предметом исследования является изучение возможности создания распределенной передачи данных с целью обеспечения повышенной устойчивости к атакам.

Практическая актуальность исследования связана с необходимостью защищенного обмена файлами по сети в условиях открытого доступа к каналам связи.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии с научно-техническим заданием и планом работ кафедры «Программное обеспечение информационных технологий» по теме «Разработать модели, методы, алгоритмы для оценки параметров, повышения надежности и качества функционирования аппаратно-программных средств систем и сетей сложной конфигурации и внедрить в современные обучающие комплексы » (ГБ № 11-2004, № ГР 20111065, научный руководитель НИР – В. В. Бахтизин).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя В. Н. Ярмолика, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на IX Международная научно-методической конференции «Дистанционное обучение – образовательная среда XXI века» в секции 4 «Информационные компьютерные сети и системы в сфере образования» (БГУИР, Минск, Беларусь, 2015) [1-А]; в научном журнале «Наука, образование и культура» в разделе «Технические науки» [2-А, 3-А].

Опубликованность результатов диссертации

По теме диссертации опубликовано 3 печатные работы, из них 1 работа в материалах конференции аспирантов, магистрантов и студентов БГУИР и 2 работы в научном журнале.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников, списка публикаций автора и приложений.

Во введение была обоснована актуальность диссертационной работы, показана необходимость использования и практическая значимость безопасных сетевых протоколов для обеспечения секретности и сохранности файлов.

В первом разделе проводится анализ предметной области. Были найдены источники информации, проведена оценка текущего этапа развития криптографии, в частности алгоритмов и методов шифрования и хеширования. Было найдено и рассмотрено семейство протоколов SSH, используемое в том числе и для безопасной передачи файлов. На основе проведенного анализа определены и сформулированы задачи к диссертационной работе.

Во втором разделе были подробно рассмотрены основные леммы и математический аппарат, на основе которого разрабатываются протоколы безопасной передачи. Основное внимание уделено математическому аппарату распределению криптографических ключей, аутентификации. Проведен

анализ математического аппарата, который был применен при реализации протокола.

Третий раздел описывает разработку и проектирование протокола передачи данных, а также требования и процесс разработки программного модуля, реализующего данный протокол.

Четвертый раздел описывает эксперименты, проведенные над протоколом. Было показано, какие дополнительные затраты приходится на распределение передачи пакетов данных. Проведено сравнение производительности с существующим протоколом SSH.

Общий объем работы составляет 81 страницу, из которых основного текста – 59 страниц, 21 рисунок на 19 страницах, список использованных источников из 22 наименований на 2 страницах и 1 приложение на 21 страницах.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

В результате работы над магистерской диссертацией разработан протокол, позволяющий организовывать безопасную передачу файлов и данных в целом по защищенным каналам, организованным в рамках данного взаимодействия.

Используя разработанный криптографический модуль были проведены экспериментальные исследования, в ходе которых было выявлено поведение протокола при использовании различных конфигураций, влияние дополнительных мер безопасности на скорость передачи данных, выявлены зависимости таких характеристик как скорость и безопасность от количества клиентских приложений в сети и числа промежуточных узлов передачи, проведено сравнение с аналогами.

Пояснительная записка состоит из 5 основных разделов.

Во введение была обоснована актуальность диссертационной работы, показана необходимость использования специфических протоколов для обеспечения целостности, аутентификации и неотрицания авторства передаваемых файлов, а также обеспечения их сохранности. Показана практическая значимость подобных протоколов в современном обществе.

В первом разделе проводится анализ предметной области. Были найдены источники информации, проведена оценка текущего этапа развития криптографии, в частности алгоритмов, методов и протоколов хеширования и шифрования, а также их применение в имеющихся сетевых протоколах транспортного уровня. Выделено и подробно рассмотрено семейство протоколов SSH. Рассмотрены и проанализированы существующие недостатки и уязвимости этих протоколов. На основе проведенного анализа определены и сформулированы задачи к диссертации.

Во втором разделе был подробно рассмотрен математический аппарат, который используется как составная часть разрабатываемых протоколов передачи данных. Основное внимание уделено математическому аппарату процесса аутентификации и схеме распределения криптографических ключей: аутентификация HMAC, алгоритм хеширования SHA-256, распределение ключей Диффи-Хелмана на основе эллиптических кривых. Проведен анализ математического аппарата, который был применен для получения заявленных свойств.

Третий раздел описывает разработку и проектирование протокола защищенной передачи файлов по распределенным каналам. Были описаны использованные протоколы сетевого уровня, процесс передачи и использование пакетов для взаимодействия с несколькими клиентами и одним сервером. Также описана разработка средства для проведения экспериментов.

Четвертый раздел описывает эксперименты, проведенные над различными конфигурациями протоколов. Было показано, какие дополнительные затраты приходятся на использование посредников при передаче файла. Проведено сравнение производительности с существующим и используемым протоколом SSH. Полученные результаты показывают, что усложнение конфигурации вносит дополнительные затраты на передачу, однако усложняют задачу взлома и перехвата сообщений для злоумышленника. Приведен анализ использования различного количества посредников при передаче, зависимость стойкости от наличия клиентов в сети. Описаны недостатки данного подхода и возможные варианты применения.

Применение подобных протоколов было описано и опубликовано на конференции «Дистанционное обучение – образовательная среда XXI века» в секции 4 «Информационные компьютерные сети и системы в сфере образования» [1-А], а также в журнале «Наука, образование и культура» в разделе «Технические науки» [2-А].

Рекомендации по практическому использованию результатов

1. Полученные результаты формируют теоретическую базу для изучения механизмов работы протоколов безопасной передачи данных.
2. Разработанный криптографический модуль может служить основой для проведения экспериментальных исследований передачи файлов от клиента серверу, а также применяться как основа для построения программного обеспечения требующего использование защищенных каналов.
3. Полученные экспериментальные данные могут послужить основой для дальнейших исследований методов и средств формирования защищенных соединений, применения их в процессе передачи файлов.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Зинькевич, В.Н. Применение безопасной передачи данных в дистанционном обучении // В.Н. Зинькевич // Дистанционное обучение – образовательная среда XXI века. Секция 4: Информационные компьютерные сети и системы в сфере обазования: Тезисы докл. – Минск : БГУИР, 2015. – с. 294 - 295.

2-А. Зинькевич, В.Н. Безопасность при передаче файлов в образовании / В.Н. Зинькевич, И.Ю. Перцев // Наука, образование и культура. Технические науки: Тезисы докл. – Москва : Издательство «Проблемы науки», 2015. – с. 7 - 9.

3-А. Перцев, В.Н. Анализ существующих угроз компьютерной безопасности в сети // И.Ю. Перцев, В.Н. Зинькевич // Наука, образование и культура. Технические науки: Тезисы докл. – Москва : Издательство «Проблемы науки», 2015. – с. 9 - 12.