Министерство образования и науки Российской Федерации

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

Кафедра теоретических основ компьютерной безопасности и криптографии

Разработка системы защищенного документооборота на базе протокола DHT

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Федоренко Вадима Станиславовича

Научный руководитель
доцент, к.ю.н. А.В. Гортинский

Заведующий кафедрой
профессор, к.ф.-м.н. В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

Сегодня трудно представить нашу жизнь без Интернета. Миллиарды людей ежедневно общаются друг с другом в Интернете, пересылают друг другу фотографии, видео и документы.

Интернет обязан своим происхождением исследованию министерства обороны США, целью которого была разработка сети, которая смогла бы сохранить свою работоспособность даже во время активных военных действий. В основе этого исследования лежала идея использования динамической маршрутизации трафика. Это гарантировало, что даже при полном уничтожении или нарушении работоспособности большей части узлов сети, сеть продолжит функционировать. Еще тогда задумывалось, что все узлы в такой сети будут равноправны, и каждый из них будет как ее автором, редактором, так и активным обозревателем, пользователем. Однако, будучи разработанным для военных нужд, Интернет со временем открылся и стал доступным всему миру. С появлением технологии «World Wide Web (W3)[1]» Интернет из военной сети превратился в сеть, заполненную различного рода медиа порталами, сервисами и прочими ресурсами, предоставляющие его пользователям те или иные услуги. Несмотря на то, что сеть Интернет первоначально задумывалась как сеть однородная, с равноправными узлами, логически сеть стала функционировать согласно архитектуре «клиент-сервер». По мере развития сетевых технологий число серверов в сети неуклонно росло, один за другим в сети появлялись сервера баз данных, DNS-сервера, почтовые сервера и т.д., но и на этом уровне взаимодействие в любой момент времени сводилось к схеме «клиент-сервер». «Интернет, который изначально был

[1] с англ. World Wide Web — Всемирная паутина, распределённая система, предоставляющая доступ к документам, расположенным на различных компьютерах, подключённых к Интернету. Всемирную паутину образуют сотни миллионов веб-серверов.

построен по неиерархической схеме, до недавнего времени на прикладном уровне использовал иерархическую схему обмена данными» [1].

Осознание того, что пользователи буквально вынуждены доверять свою информацию обезличенным корпорациям в сети, сервера, центральные точки которой в любой момент времени подвержены риску выйти из строя или быть уничтоженными в процессе внешнего воздействия или вторжения, привело к появлению «peer-to-peer» сетей. Первое упоминание о термине «peer-to-peer» датировано 1984 годом [2]. В этом году компания IBM представила миру новую сетевую архитектуру, которая позволяла осуществлять динамическую маршрутизацию трафика независимо от топологии компьютерной сети. Несмотря на кажущуюся революционность, технология «peer-to-peer» — это не более чем надстройка над уже имеющимися, изначально заложенными в сеть Интернет, технологиями. Как и задумывалось при разработке сети Интернет, такая архитектура сети основывалась на условии полного равноправия всех её участников. Подобная архитектура сети называется пиринговой (или одноранговой), а узлы такой сети – пирами [3].

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В разделе «Пиринговые сети» представлен краткий экскурс в теорию пиринговых сетей, рассмотрены ее архитектура и классификации, а также наиболее популярные протоколы, которые определяют, непосредственно, работу самих пиринговых сетей.

В разделе «Система защищенного документооборота на базе протокола DHT» демонстрируется разработанный программный продукт, предназначенный для защищенного документооборота в пиринговых сетях на основе протокола DHT. Описываются краткие характеристики этого программного продукта.

Далее, следует раздел «Описание использованных в реализации системы защищенного документооборота технологии», в котором последовательно описаны наиболее важные технологии, лежащие в основе реализации приложения защищенного документооборота в пиринговых сетях, а именно «Пиринговый протокол DHT Kademlia», «Стандарт шифрования OpenPGP» и «Клиент-серверная архитектура REST». Следом за этим разделом идет описание «Структуры системы защищенного документооборота». В разделе представлены основные компоненты, обеспечивающие и поддерживающие работу всей системы в целом: это «Сервер-координатор» и «Клиент системы защищенного документооборота».

Предварительно ознакомившись с приложением, предлагается разобраться как работать с ним, о чем рассказывается в разделе «Описание процесса работы с системой защищенного документооборота». В разделе представлены такие этапы работы с приложением, как «Установка», «Запуск», «Авторизация», «Регистрация», «Добавление/удаление друзей», «Предоставление документов пользователям» и «Загрузка документов».

Впоследствии демонстрируются основные подходы, которые используются приложением. В отличие от предыдущих разделов,

описывающих и знакомящих с системой документооборота, в разделе «Описание использованных подходов в реализации системы защищенного документооборота» приведена информация конкретно о самой реализации приложения в детальном формате, приближенном к уровню кода. В нем описаны «Структура открытого и секретного ключей», «Структура распределенной таблицы хешей DHT» и, непосредственно, «Процесс передачи документов».

ЗАКЛЮЧЕНИЕ

Технологии, лежащие в основе современных пиринговых сетей, представляют собой весьма сложные, но порой элегантные и эффективные решения. Однако, такая сложность вполне оправданна, поскольку польза, полученная при использования подобных сетей несравнима с затраченным временем на их разработку. Эти сети только начали набирать популярность. В нынешних условиях жесткого контроля и цензуры в Интернете необходимость в таких сетях резко возрастает.

В ходе работы был выполнен обзор пиринговых сетей, дана их классификация и рассмотрены наиболее часто используемые протоколы, лежащие в их основе, а также разработан программный продукт для защищенного документооборота в пиринговых сетях на основе протокола DHT.

Программный продукт, представленный в работе, одинаково хорошо и эффективно справляется как с шифрованием документов, так и с их передачей, и может получить широкое распространение в областях, связанных с наукой или бизнесом, там, где потраченное время и безопасность информации ценятся превыше всего.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. A Definition of Peer-to-Peer Networking for the Classification of Peer-toPeer Architectures and Applications [Электронный ресурс] // R¸diger Schollmeier, Institute of Communication Networks, Technische Universit‰t Munchen. URL: http://www.computer.org/csdl/proceedings/p2p/2001/1503/00/15030101.pdf (дата обращения 11.10.2015)
2. Алгоритмы и применения сетей P2P [Электронный ресурс] // Интуит. Национальный открытый университет. URL: http://www.intuit.ru/studies/courses/9/9/lecture/279?page=4 (дата обращения 14.10.2015)
3. Collaborative Applications over Peer-to-Peer Systems – Challenges and Solutions". Peer-to-Peer Networking and Applications [Электронный ресурс] // H. M. N. Dilum Bandara and Anura P. Jayasumana Colorado State University, Fort Collins. URL: http://arxiv.org/ftp/arxiv/papers/1207/1207.0790.pdf (дата обращения 14.10.2015)
4. Peer-to-Peer Computing [Электронный ресурс] // D. Barkai., Intel Press, URL: http://www.edb.utexas.edu/minliu/multimedia/PDFfolder/PeerComputing.pdf (дата обращения 14.10.2015)
5. Применение сетей P2P [Электронный ресурс] // Семенов Ю.А. (ИТЭФ-МФТИ). URL: http://book.itep.ru/4/41/p2p.htm (дата обращения: 14.10.2015).
6. Peer-to-peer [Электронный ресурс] // From Wikipedia, the free encyclopedia URL: https://en.wikipedia.org/wiki/Peer-to-peer (дата обращения: 12.10.2015). https://ru.wikipedia.org/wiki/оверлейная_сеть
7. Одноранговая сеть [Электронный ресурс] // Материал из Википедии — свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/Одноранговая_сеть (дата обращения: 12.10.2015).

8. Пиринговые сети [Электронный ресурс] // Интернетика. Навигация в сложных сетях: модели и алгоритмы. URL: http://bourabai.kz/dbt/internetica/piring.htm (дата обращения: 3.12.2015).
9. Анонимная связь в пиринговых сетях для улучшения приватности и безопасности [Электронный ресурс] // Ehsan Saboori and Shahriar Mohammadi. URL: http://markelov.biz/Proekty/Kursovye/Komp'juternyesetiBSOD/files?get=anonymous_communication_in_peertopeer_networks.pdf (дата обращения: 3.12.2015).
10. Kademlia DHT: Основы [Электронный ресурс] // IT-сообщество. URL: http://habrahabr.ru/post/107342/ (дата обращения: 12.10.2015).
11. Маршрутизация в пиринговых сетях [Электронный ресурс] // Хлюпин Ф. С. (Москва, Московский государственный технологический университет «СТАНКИН», Россия). URL: http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=14&pa=4&ar=1 (дата обращения: 13.10.2015)
12. Gnutella [Электронный ресурс] // Материал из Википедии — свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/Gnutella (дата обращения: 18.11.2015)
13. Freenet [Электронный ресурс] // Материал из Википедии — свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/Freenet (дата обращения: 18.11.2015)
14. Распределённая хеш-таблица [Электронный ресурс] // Материал из Википедии — свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/Распределенная_хеш-таблица.(дата обращения: 18.11.2015)
15. Kademlia [Электронный ресурс] // Материал из rfwiki. URL: http://ru.rfwiki.org/wiki/Kademlia (дата обращения: 21.11.2015)
16. Kademlia: A Peer-to-peer information system based on the XOR Metric [Электронный ресурс] // Petar Maymounkov and David Mazieres. URL:

https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf (дата обращения: 28.11.2015)

17. Что такое PGP [Электронный ресурс] // PGP в России. URL: https://www.pgpru.com/faq/obschie (дата обращения: 30.11.2015)
18. PGP [Электронный ресурс] // Материал из Википедии — свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/PGP (дата обращения: 30.11.2015)
19. REST [Электронный ресурс] // Материал из Википедии — свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/REST (дата обращения: 1.12.2015)
20. PGP [Электронный ресурс] // Crypto wiki. URL: http://cryptowiki.net/index.php?title=PGP (дата обращения: 10.12.2015)