УДК 004.41.42

А. М. Шитько, Н. В. Пацей
Белорусский государственный технологический университет

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА PEER-TO-PEER ДЛЯ ЗАЩИЩЕННОГО ОБМЕНА ДАННЫМИ

Статья посвящена структуре и разработке системы защищенного обмена данными по протоколу peer-to-peer (P2P), с помощью которого формируется оверлейная компьютерная сеть, основанная на равноправии участников. Разработанная система состоит из двух компонент: сервера, необходимого для координации участников в сети и передачи данных между ними, размещенного в глобальной сети Интернет, и клиента (пир), который представляет собой приложение на платформе Android для работы в P2P-сети. Рассмотрены методы и алгоритмы шифрования, необходимые для защиты входящего и исходящего трафика, проанализированы наиболее распространенные и криптостойкие в изучаемой области. Исследована работа P2P-протокола, описаны принципы защиты данных в P2P-сети, их хранение в базе данных и передача по сети между устройствами Android. Также проведен анализ преимуществ разработанной системы, ее недостатков и способов их устранения. Результатом выполненного исследования является разработанный веб-сервер для организации P2P-сети и маршрутизации участников в ней, а также программное средство на платформе Android для работы в данной сети и защищенной передачи данных по P2P-протоколу.

Ключевые слова: peer-to-peer, шифрование, защита данных, Android, Spring, OAuth.

A. M. Shit'ko, N. V. Patsei
Belarusian State Technological University

PROTECTED DATA EXCHANGE ON BASE PEER-TO-PEER PROTOCOL

The article focuses on the structure and development of the system for protected data exchange according to the peer-to-peer (P2P) protocol. It is used to organize the overlay computer networks based on equality of participants. The developed system consists of two components: the server necessary for participants coordination in networks and data transfers, placed on the wide area network the Internet, and the client (peer) – Android platform application for operation in P2P network. The methods and encryption algorithms necessary for protection of the entering and originating traffic are considered in the article. The most widespread cryptographic system in the researched area are analyzed. The principles of data security in P2P network, their storage in a database and transmissions between Android devices are described. The analysis of developed system advantages, its shortcomings and methods of their elimination is also carried out. The result of the research is the developed Web-server for the peer-to-peer network organization and routing of participants in it; Android platform software for operation on this network and protected data transfer through P2P protocol.

Key words: peer-to-peer, encoding, data security, Android, Spring, OAuth.

Введение. Число разновидностей зловредных мобильных программ увеличилось с нескольких сотен до десятков тысяч. Всеобщая распространенность и популярность мобильных устройств приводит к чрезвычайной актуальности проблемы обеспечения безопасности мобильных приложений. Поскольку в таких устройствах хранятся большие объемы личной информации, они являются привлекательными целями для атак злоумышленников, стремящихся к получению финансовой выгоды. По статистике примерно половина атак ориентирована на кражу личных данных и отслеживание поведения пользователей. Ситуация осложняется и тем, что мобильные устройства обладают сравнительно небольшой вычислительной мощностью и ограниченным пользовательским интерфейсом, что позволяет злоумышленникам скрывать от пользователей активность зловредных программ.

На данный момент основной целью кибератак являются мобильные устройства на платформе Android. С их помощью люди общаются, передают различные файлы, совершают платежи и многое другое. При передаче данных люди хотят быть уверенными в том, что данная информация будет конфиденциальной. Поэтому важным становится разработка приложений с определенным уровнем защиты информации.

На сегодняшний день одним из вариантов защиты передаваемых данных между мобильными устройствами является использование протокола peer-to-peer. Peer-to-peer (коротко P2P) – протокол, позволяющий организовать прямую связь между индивидуальными устройствами и установить ряд сетевых принципов

разработки. Фактическое определение того, что такое P2P, варьируется у различных авторов, но большинство согласно с тем, что P2P-система отвергает клиент-серверную модель и основана на равноправии участников. Такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов [1].

К ключевым характеристикам P2P-сетей относятся:

1) управляемость – простота поддержания работоспособности системы, а также решения вопросов, связанных с обновлением, восстановлением после сбоев и регистрацией активности (logging);

2) информационная согласованность – достоверность, проверяемость и последовательность информации;

3) расширяемость – возможность расширения информационных ресурсов системы;

4) устойчивость к сбоям – надежность системы;

5) безопасность – степень защиты информации от несанкционированного доступа;

6) устойчивость к внетехнологическому вмешательству – возможность (или невозможность) вмешательства государственных и иных органов в работу сети ввиду каких-либо причин (например, обвинение в нарушении авторских прав);

7) масштабируемость – наличие пределов (как правило, технологических) увеличения мощностей и предельная стоимость расширения.

Существует два типа P2P-сети: децентрализованная, основанная на равноправии участников (пиров), т. е. выполняет функции и клиента, и сервера; и частично децентрализованная (гибридная), в которой существует сервер, используемый для координации, поиска или предоставления информации о существующих участниках сети и их статусе (online, offline и т. д.). В разрабатываемой системе применялся гибридный тип сети.

Основная часть. В системе защищенного обмена данными использовались следующие криптографические алгоритмы:

– AES – симметричный алгоритм шифрования, длина ключа – 256 бит; применяется для шифрования каждого файла или сообщения;

– SHA-2 – функция хеширования, длина дайджеста сообщения – 256 бит; используется для вычисления приватного ключа хешированием данных пользователя (имя и идентификатор), а также некоторых вспомогательных данных (salt);

– PRNG – генератор псевдослучайных последовательностей для криптографического применения; используется для генерации ключа алгоритма шифрования AES;

– шифр Эль-Гамаля на эллиптических кривых (ЭК) – алгоритм асимметричного шифрования, длина ключа – 256 бит; применяется в качестве криптографического контейнера для передачи ключа алгоритма шифрования AES от одного пользователя к другому.

Для защищенного обмена сообщениями использовалась гибридная система шифрования. Так, процедуры шифрования выполнялись при помощи криптоалгоритма AES, а передача ключевых данных осуществлялась на основе шифра Эль-Гамаля на ЭК.

Структурно система представляет собой два компонента: клиентский и серверный. Сервер разработан на языке Java с использованием Spring Framework. Данная библиотека представляет собой облегченную платформу для построения Java-приложений, что позволяет создавать любой тип приложений с минимальными усилиями и делать их более производительными и отказоустойчивыми [2]. Для реализации P2P-протокола применялась библиотека JXTA, которая представляет собой спецификацию протоколов по обслуживанию P2P-сетей для обмена данными различного типа. Также на сервере установлен SSL-сертификат для организации защищенного соединения с участниками сети. Сервер размещен на хостинге Google App Engine для возможности доступа к нему из глобальной сети Интернет. Вся передаваемая информация хранится в Google Cloud SQL, которая представляет собой реляционную базу данных, находящуюся в «облаке» Google. Данные в базе удаляются после окончания сеанса работы.

Для организации обмена данными между мобильными устройствами, а также их маршрутизации в глобальной сети Интернет необходимо пройти регистрацию в P2P-сети. Важным преимуществом системы является упрощенная (для пользователя) регистрация на основе протокола авторизации OAuth 2.0. Особенность его в том, что он позволяет выдавать права на доступ к ресурсам пользователя без предоставления логина и пароля. Вместо этого каждый пользователь получает «токен» доступа, который является результатом авторизации и пропуском к защищенному ресурсу [3]. К преимуществам протокола OAuth относятся:

1) безопасность – при разработке приложения не нужно заботиться об обеспечении конфиденциальности логина и пароля пользователя. Логин и пароль не передаются приложению, а следовательно, не могут попасть в руки злоумышленников. Также безопасность достигается путем использования SSL, что сильно упрощает разработку;

2) доверие – у пользователя больше оснований доверять приложению, поскольку пользователь

может быть уверен, что несанкционированный доступ к его личным данным невозможен. Не владея логином и паролем пользователя, приложение сможет выполнять только те действия с данными, которые разрешил пользователь, и никакие другие;

3) удобство для пользователей – если сам пользователь уже авторизован на сервисе, ему не нужно вводить логин и пароль повторно перед выдачей разрешения приложению. Отсутствие частого ввода логина и пароля особенно актуально для пользователей мобильных приложений.

Поскольку сейчас большинство пользователей зарегистрировано в социальных сетях, в данной системе используется OAuth-сервер социальных сетей «ВКонтакте» и «Facebook», что позволяет зарегистрировать пользователей на сервере с персональными данными, полученными с указанных социальных сетей. Процедура регистрации представлена на рис. 1.

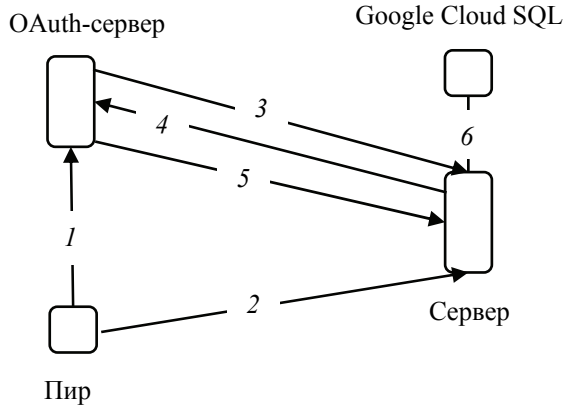

Рис. 1. Схема регистрации в сети

В ходе регистрации пир посылает get-запрос на OAuth-сервер *1*, в теле которого содержатся идентификатор клиента, предварительно полученный от сервера социальной сети, URL-перенаправления, на который будет направлен пользователь после успешной авторизации, и тип ответа, равный «code», для получения кода от сервера, с помощью которого генерируется «токен» доступа. Дополнительно для пользователя создается универсальный уникальный идентификатор *2*, который генерируется средствами библиотеки JXTA при создании объекта «Peer» и отсылается на Spring-сервер. Он необходим для поиска участника в сети и передачи ему информации. После успешной авторизации на Spring-сервер отсылается «code» *3*. Далее для получения «токена» доступа с сервера посылается get-запрос *4* с такими параметрами, как идентификатор клиента, секретный ключ, предварительно полученный от сервера социальной сети, код и URL-перенаправления. После чего на разрабатываемый сервер приходит ответ *5* в формате JSON с «токеном» доступа и идентификатором пользователя. Для получения персональных данных пользователя необходимо сделать еще один запрос на объект «users.get», вследствие чего возвращается ответ в формате JSON с персональными данными клиента. Все полученные данные сохраняются в базе данных *6* на сервере, после чего регистрация пользователя в сети завершается.

Теперь рассмотрим непосредственно сам процесс обмена информацией. В JXTA данные передаются по двунаправленным именованным каналам, что является преимуществом по сравнению со стандартными каналами: нет необходимости создавать отдельно каналы для чтения и записи, эти функции берет на себя один канал, описанный в спецификации JXTA. Схема процесса передачи приведена на рис. 2.

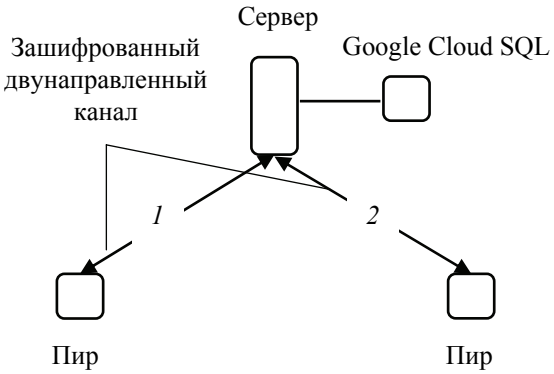

Рис. 2. Схема передачи сообщений

Пир отправляет сообщение по каналу на сервер с указанием UUID адресата *1*, оттуда оно доставляется адресату с соответствующим уникальным идентификатором *2*. Для защиты передаваемых данных в системе будем использовать зашифрованные двунаправленные именованные каналы, которые позволяют обезопасить данные от несанкционированного доступа, а также предотвратить их перехват и изменение. Защита данных в таких каналах осуществляется за счет использования криптографического протокола TLS, который обеспечивает защищенную передачу данных между узлами в сети Интернет. В спецификации JXTA максимальный размер передаваемой информации по именованному двунаправленному каналу составляет 8 Кб, что делает невозможным передачу файлов размером больше указанной величины, поэтому по каналу будут передаваться только сообщения. Как следствие, передача файлов будет осуществляться с помощью https-протокола. Данный процесс имеет схожую структуру со схемой передачи сообщений и представлен на рис. 3.

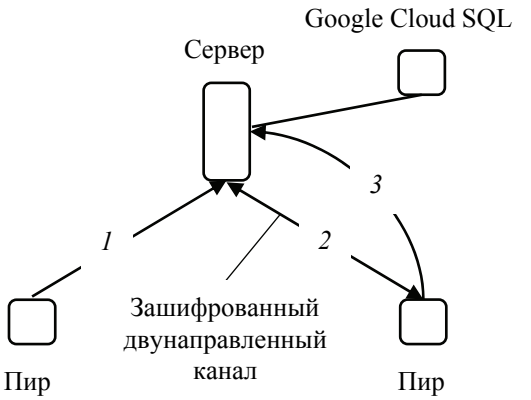

Рис. 3. Процесс передачи файлов

Пир по протоколу https отправляет файл вместе с UUID адресата на сервер *1*, а сервер по каналу *2* отправляет адресату ссылку на этот файл, что позволяет инициировать автоматический запрос *3* этого файла с сервера или запрос по требованию.

Заключение. Таким образом, выполнена разработка серверного компонента системы защищенного обмена данными между мобильными устройствами, который основан на библиотеке Spring, с помощью протокола OAuth 2.0 регистрирует всех участников в сети и координирует их работу. Разработано также клиентское приложение на платформе Android, позволяющее отправлять данные по защищенному каналу всем доступным адресатам по протоколу peer-to-peer. К преимуществам предложенной системы можно отнести:

– удобство использования;

– упрощенная для пользователей регистрация;

– защита передаваемой информации с помощью гибридной системы шифрования.

Существенным недостатком системы является проблема масштабируемости, так как используется гибридный тип P2P-сети и основная нагрузка приходится на сервер. Однако эта проблема возникает только в случае значительного увеличения размеров пир-сети, вследствие чего сервер не сможет справляться с большим количеством запросов. Данная задача решается вводом дополнительных серверов.

Литература

1. Verstrynge J. Practical JXTA II. Cracking the P2P puzzle. Netherlands: DawningStreams Publ., 2010. 271 p.

2. Ho Cl., Harrop R. Pro Spring 3. USA: APress, 2012. 871 p.

3. Boyd R. Getting Started with OAuth 2.0. USA: O'Reilly Media Publ., 2012. 65 p.

References

1. Verstrynge J. Practical JXTA II. Cracking the P2P puzzle. Netherlands, DawningStreams Publ., 2010. 271 p.

2. Ho Cl., Harrop R. Pro Spring 3. USA, APress, 2012. 871 p.

3. Boyd R. Getting Started with OAuth 2.0. USA, O'Reilly Media Publ., 2012. 65 p.

Информация об авторах

Шитько Андрей Михайлович – магистрант, ассистент кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: a.shitko@belstu.by

Пацей Наталья Владимировна – кандидат технических наук, доцент, доцент кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: n.patsei@belstu.by

Information about the authors

Shit'ko Andrey Mikhaylovich – undergraduate, assistant, the Department of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: a.shitko@belstu.by

Patsei Natallia Vladimirovna – Ph. D. (Engineering), Assistant Professor, Assistant Professor, the Department of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: n.patsei@belstu.by

Поступила 12.03.2015