УДК 004.05+004.7

магистр Е.А. Правда
ГВУЗ «Национальный горный университет»

ФАЙЛООБМЕННЫЕ ПИРИНГОВЫЕ СЕТИ И ИХ ОСНОВНЫЕ УЯЗВИМЫЕ СТОРОНЫ

В работе представлено устройство сетей построенных по технологии Peer-to-peer. Рассмотрены их основные уязвимости и методы защиты.

По мере развития Интернета все больший интерес у пользователей вызывают технологии обмена файлами. Более доступная, чем раньше, Сеть и наличие широких каналов доступа позволяют значительно проще находить и закачивать нужные файлы. Не последнюю роль в этом процессе играют современные технологии и принципы построения сообществ, которые позволяют строить системы, весьма эффективные с точки зрения, как организаторов, так и пользователей файлообменных сетей. По некоторым данным, в настоящее время в Интернете более половины всего трафика приходится на трафик файлообменных пиринговых сетей. Размеры самых крупных из них перевалили за отметку в миллион одновременно работающих узлов. Общее количество зарегистрированных участников таких файлообменных сетей во всем мире составляет более 100 млн.

Peer-to-peer (P2P) технологии являются одной из наиболее популярных тем на сегодняшний день. Популярность, достигнутая с помощью таких программам как Skype, Bittorrent, DirectConnect и список таких программ можно продолжать и продолжать, подтверждает потенциал peer-to-peer систем.

Работа в типичной файлообменной сети строится следующим образом:

– Клиент запрашивает в сети требуемый файл (перед этим возможно проведя поиск нужного файла по данным, хранящимся на серверах).

– Если нужный файл имеется и найден, сервер отдает клиенту IP-адреса других клиентов, у которых данный файл был найден.

– Клиент, запросивший файл, устанавливает «прямое» соединение с клиентом или клиентами, у которых имеется нужный файл, и начинает его скачивать (если клиент не отключен в это время от сети или не перегружен).

Сети, созданные на основе технологии Peer-to-Peer, также называются пиринговыми, одноранговыми или децентрализованными. И хотя они используются сейчас в основном для разделения файлов, существует еще много других областей, где данная технология тоже успешно применяется. Это телевидение и аудиотрансляции, параллельное программирование, распределенное кэширование ресурсов для разгрузки серверов, рассылка уведомлений и статей, поддержка системы доменных имен, индексирование распределенных ресурсов и их поиск, резервное копирование и создание устойчивых распределенных хранилищ данных, обмен сообщениями, создание систем, устойчивых к атакам типа “отказ в обслуживании”, распространение программных модулей.

Реализация и использование распределенных систем имеют не только плюсы, но и минусы, связанные с особенностями обеспечения безопасности. Получить контроль над столь разветвленной и большой структурой, какой является сеть P2P, или использовать пробелы в реализации протоколов для собственных нужд — желанная цель для хакеров. К тому же защитить распределенную структуру сложнее, чем централизованный сервер.

Столь огромное количество ресурсов, которое имеется в сетях P2P, тяжело шифровать/дешифровать, поэтому большая часть информации об IP-адресах и ресурсах участников хранится и пересылается в незашифрованном виде, что делает ее доступной для перехвата. При перехвате злоумышленник не только получает собственно информацию, но также узнает и об узлах, на которых она хранится, что тоже опасно.

Только в последнее время в клиентах большинства крупных сетей эта проблема стала решаться путем шифрования заголовков пакетов и идентификационной информации. Появляются клиенты с поддержкой

технологии SSL, внедряются специальные средства защиты информации о местонахождении ресурсов и пр.

Серьезная проблема — распространение “червей” и подделка ID ресурсов с целью их фальсификации.

Чтобы справиться с описанной проблемой, клиенты должны пользоваться надежными хеш-функциями (“деревьями” хеш-функций, если файл копируется по частям), такими, как SHA-1, Whirlpool, Tiger, и только для решения малоответственных задач — контрольными суммами CRC. Для уменьшения объемов пересылаемых данных и облегчения их шифрования можно применить компрессию. Для защиты от вирусов нужно иметь возможность хранить идентифицирующую метаинформацию о “червях”, как это, в частности, сделано в сети Gnutella2.

Другая проблема — возможность подделки ID серверов и узлов. При отсутствии механизма проверки подлинности пересылаемых служебных сообщений, например с помощью сертификатов, существует возможность фальсификации сервера или узла (многих узлов). Так как узлы обмениваются информацией, подделка некоторых из них приведет к компрометации всей сети или ее части. Закрытое ПО клиентов и серверов не является решением проблемы, так как есть возможность обратного инжиниринга протоколов и программ (reverse engineering).

В настоящее время выделенные серверы и узлы периодически обмениваются между собой верифицирующей информацией и при необходимости добавляют поддельные серверы/узлы в черный список блокировки доступа.

Также ведется работа по созданию проектов, объединяющих сети и протоколы (например, JXTA – разработчик Билл Джой).

Перечень литературы:

1. http://wiki.a42.ru/index.php/Безопасность_в_p2p
2. Ю. Н. Гуркин, Ю. А. Семенов. «Файлообменные сети P2P: основные принципы, протоколы, безопасность» // «Сети и Системы связи»

3. http://style-hitech.ru/peer-to-peer_i_tjekhnologii_fajloobmjena