

## Ipo4ta. Новый почтовый протокол.

Стефанов Слава, @ipo4ta.com/admin  
08.11.06

Протокол SMTP устарел. Эффективность электронной почты, основанной на этом протоколе, сегодня порядка 30% поскольку около 70% процентов всех передаваемых сообщений составляет спам. Из-за "мусорных" рекламных рассылок почта пересылает в основном то, что нежелательно для конечного пользователя.

Как можно побороть спам?

Чтобы получатель однозначно определил спам ему необходимо просмотреть сообщение. Автоматические фильтры помогают в разгребании мусора, но не решают саму проблему. Причем из-за наличия спам-фильтров спамер вынужден увеличивать объем рассылок чтобы что-то просочилось сквозь фильтры.

Смысл рекламы через спам в дешевизне рассылки сообщений. При крайне низком проценте отклика на такую рекламу, спам остается выгодным именно за счет дешевизны.

Появлялись сообщения о разработке технологии "электронных марок" наподобие марок в оффлайновой почте, когда отсылающий платит за пересылку. Эта идея тихо-мирно канула в лету. Логически рассуждая так и должно было быть, ведь фактически идея состояла в искусственном удорожании для любого пользователя услуги, реальная стоимость которой очень низка.

Вообще, прямое копирование "оффлайновой" модели в сетевую технологию не всегда лучшее решение. Например протокол SMTP по сути копирует поведение обычной почты : отправляя сообщение вы "приносите" ваше письмо на ваш локальный "почтовый узел" и затем сообщение физически(!) переносится на "почтовый узел" получателя. Получатель "забирает" письмо со своего "почтового узла". Именно так работает традиционная почта ("заказное письмо" или что-то вроде того).

В этой схеме единственный функциональный параметр, участвующий в процессе передачи сообщения это адрес получателя. Поэтому так легко спамерам безнаказанно подделывать адрес отправителя, не опасаясь волны возмущенных ответов. Адрес отправителя не участвует в работе протокола и он не важен для доставки письма по назначению. Конечно во времена создания SMTP никто не подозревал о возможности такой проблемы. Но теперь она есть и с этим надо что-то делать.

Итак мы видим две проблемы современной е-почты. Одна из них техническая : **проблема идентификации отправителя**. Вторая скорее организационная - как ограничить спамера и **сделать для него массовые рассылки рекламного мусора неэффективными**.

**Обе эти проблемы решены в системе Ipo4ta (и-почта, интернет-почта).**

Рассмотрим первую: **идентификация отправителя**. В системе Ipo4ta сообщение не переносится целиком с сервера отправителя на сервер получателя в момент отправки. Письмо остается на сервере отправителя, пересылается лишь уведомление, содержащее идентификатор сообщения и адрес отправителя, который в то же время является адресом физического нахождения сообщения в сети. Открывая сообщение пользователь дает команду системе запросить данные с адреса отправителя пользуясь уникальным идентификатором как ключем доступа. Оба параметра (адрес отправителя и ключ) содержатся в уведомлении. При этом вся процедура проходит совершенно прозрачно для пользователя, его действия такие же как в случае обычного email.

Мы видим, что адрес отправителя становится функциональной частью протокола и если он неверен, то сообщение не может быть получено в принципе, ведь для получения сообщения необходимо "забрать" его с сервера-отправителя, предъявив уникальный идентификатор сообщения. Этот подход также уменьшает неэффективный трафик, поскольку если пользователь удалит сообщение (точнее уведомление) не пытаясь его открыть, то сообщение не будет запрошено с сервера отправителя.

Этот подход превращает систему Ipo4ta из системы обмена сообщениями в нечто гораздо большее.

Посмотрим на нее повнимательнее. Итак пересылая сообщение мы оставляем письмо, т. е. некий "файл" Ф лежать на сервере отправителя, а другой, совсем маленький файл "уведомление" У отправляется на сервер получателя. Какую роль играет для получателя "уведомление", содержащее уникальный идентификатор сообщения? Фактически для получателя этот файл является ключом для получения основного файла Ф с сервера отправителя. Значит в системе Ipo4ta пользователь имеет возможность пересылать другим "ключи", открывающие доступ к файлам в его папке на почтовом сервере! Рассылая друзьям "уведомления" я просто даю им ключи доступа к своему файлу. Причем система должна помнить кому эти ключи были отправлены, то есть кто именно имеет права на получение файла Ф.

*Техническое замечание : в реализации системы Ipo4ta есть 2 основных типа передаваемых объектов – сообщения и файлы (присоединенные файлы), доступ к файлам в системе Ipo4ta осуществляется посредством базового протокола в интернет - HTTP, обмен сообщениями происходит с помощью протокола SOAP (веб-сервис).*

Мы видим что система Ipo4ta естественным образом содержит в себе подсистему контроля доступа к файлам каждого пользователя. Причем пользователь волен этими правами распоряжаться и передавать другим. В Ipo4ta мы расширили эту подсистему так, чтобы пользователь мог управлять правами доступа не только к файлам, но и к папкам. Кроме того добавили к уже указанному нами праву "получение файла" (назовем его правом "чтение") еще права "создание/получение сообщения/файла" (назовем его правом "запись") и право "отправка" для отправки сообщений.

Правом "отправка" обладает например владелец папки. А остальные права он может раздавать по своему усмотрению. Предположим что пользователь решил для некоторой своей папки по имени WWW, установить право "чтение" вообще для всех желающих. Мы получили некоторую папку с файлами, доступными по протоколу

HTTP всякому желающему. Ничего не напоминает? Мы получили вебсайт( домашнюю страницу ) пользователя системы Ipo4ta как естественную часть системы.

Двинемся дальше и создадим еще одну папку, назовем ее ФОРУМ, для которой разрешим не только чтение, но и запись. Запись разрешим например только тем, кто имеет почтовый адрес в системе Ipo4ta. В системе есть возможность автоматической проверки идентичности пользователя между почтовым сервером пользователя и всеми остальными почтовыми серверами. Итак, если сторонний пользователь получает доступ к этой папке он может не только читать сообщения но и создавать новые. Мы получили персональный интернет-форум (можно его понимать также как "блог") пользователя системы Ipo4ta.

Ну и последнее, папка ВХОДЯЩИЕ. Разрешение для всех только одно "запись". В такой конфигурации получаем папку для входящих сообщений.

Незначительно расширяя исходный протокол мы пришли к системе, объединяющей в одно целое почту, домашнюю страницу и личный форум.

Причем из-за возможности идентификации пользователя между почтовыми серверами отпадает необходимость всякий раз регистрироваться в форумах. Пользователь входит со своим паролем в свой ящик а далее может перемещаться в чужие форумы напрямую. Доступ будет получен на основании "договора" между почтовыми серверами прозрачно для пользователя.

Пришло время разобраться со второй проблемой, **проблемой спама**. Мы не можем открыть доступ "запись" к папке ВХОДЯЩИЕ только для "хороших". Технология пока не настолько хорошо развита, так что нам придется искать другие пути. Например можно открыть папку на "запись" только для друзей из моей адресной книги. Но тогда никто другой написать не сможет. А это письмо от "другого" может быть крайне важно. Всякий должен иметь возможность написать мне, иначе почта теряет смысл.

Можем ли мы использовать как-то идею "электронных марок"? Ведь в ней определенно есть здоровое зерно. Если спамер должен за каждое отправленное письмо заплатить денег, то рассылка миллионов писем выйдет ему в копеечку и перестанет быть эффективной. Но в случае "электронных марок" и я должен буду платить за отправку письма моему другу. Это совсем не логично поскольку большинство наших сообщений мы пишем друзьям/знакомым. Да и спрашивается – кому я буду платить за эти самые "марки"?

Похоже, иначе чем включить деньги в почтовый оборот спамера не победить. Но можно ли сделать так, чтобы спамер платил, а я - нет? Решение существует и оно весьма простое. Во первых, плату нужно брать не за пересылку ( таков смысл "электронных марок" ) а за получение мною письма в мой почтовый ящик. И во вторых, плату эту должен получать я сам. А раз я буду получать эту плату то я должен иметь возможность установить размер этой платы. И затем, я должен иметь возможность одним щелчком мыши отменять полученную мною за входящее письмо плату, если это письмо от "правильного" корреспондента.

Делались попытки встроить похожие методы в SMTP протокол. Такие системы существуют но из-за особенностей SMTP протокола действуют они.. непрямым

путем в общем. Сложно получается. В случае Ipo4ta внедрить метод "плата за входящие" для "страхования" сообщения получается совершенно естественным образом.

А именно : в системе Ipo4ta, определяя право на запись в папку, пользователь устанавливает дополнительный параметр "цена". Скажем, для записи в папку ВХОДЯЩИЕ, пользователь определяет такие правила : для всех из моей адресной книги право на запись с ценой 0 ("свои" не платят); для всех остальных установим небольшую цену. Если получено письмо от "своего", пользователь щелкает на кнопку "отменить платеж" и заносим новый контакт в адресную книгу. В случае спамерских сообщений плату берем, сообщение удаляем.

Рассмотрим как действует механизм платежей более детально. Предположим у всех участников сценария установлена плата за входящие сообщения для всех незнакомцев. Когда обычные пользователи, знакомые/приятели, обмениваются сообщениями в первый раз, то получив сообщения, они отменяют платежи друг друга и никаких расходов у них в результате нет. Они сразу добавляют друг-друга в адресную книгу и переписываются в дальнейшем бесплатно. Если сообщения деловые, то возможно отменять платеж получатель и не станет, но в ходе переписки взаимные платежи компенсируются. Внакладе остается только тот, кто много сообщений отправляет и мало получает, это и есть спамер.

Еще один интересный аспект проблемы : сегодня очень часто спамер пользуется для рассылки сообщений "зомбированными" компьютерами. Т. е. с помощью вирусов/троянских программ спамер получает административный доступ к компьютеру-жертве и в дальнейшем этот компьютер используется для рассылок спама. В случае Ipo4ta опасность использования таких машин "зомби" снижается. Если злоумышленник получил возможность рассылать письма от имени пользователя, то отправить много писем не удастся просто потому что за отправленные письма придется платить со счета пользователя, а на счету не может быть неограниченно много денег (это легко контролировать).

Работы над протоколом и системой Ipo4ta еще не завершены. Но версия 0.7 уже готова и функционирует. Система включает в себя спецификацию протокола, серверное и клиентское(веб-интерфейс) программное обеспечение, написанное на языке JAVA. Ipo4ta это проект с открытым кодом, распространяемый под лицензией GPL. Доступны версии с русским и английским интерфейсами.

Мы надеемся что эта статья вызовет интерес к проекту Ipo4ta, и что найдутся желающие тестировать, использовать, критиковать и развивать наш проект вместе с нами. Детали на сайте [ipo4ta.com](http://ipo4ta.com).