Р. Богатырев

Простая защита от спама.
Принцип сталинской вертушки

Принцип, который здесь будет рассмотрен, не претендует на панацею от "информационной чумы XXI века". Он не отрицает иных организационных, технологических и правовых мер [1]. В то же время принцип крайне прост и весьма эффективен. Причем полезен как индивидуальным, так и корпоративным пользователям. Чем примечателен этот способ — он практически сводит к нулю ухищрения спаммеров, постоянно совершенствующих свои методы борьбы с "войсками" антиспамовой коалиции.

Классификация спама

Поскольку спам представляет собой нежелательную корреспонденцию, доставляемую по каналам электронной почты, то нечеткость понимания степени "нежелательности" и приводит к тому, что бороться со спамом непросто. В самом деле, тремя наиболее распространенными видами спама являются реклама, агитация и хулиганство. В рекламе и агитации иногда содержится полезная информация, поэтому заведомо отметать такие потоки спама неразумно. Что касается хулиганства, нередко сопровождаемого угрозами, обвинениями и т.п., то оно требует жесткого заслона, дабы отправитель не смог добиться своих целей (включая и желание попортить нервы).

Рассмотрим два родственных для электронной почты средства коммуникаций: телевидение и телефонную связь. В случае телевидения прямым аналогом спама является реклама. Бороться с рекламными блоками можно либо организационными мерами (переключая каналы и зная ориентировочную продолжительность блоков), либо технологическим путем (определяя и "вырезая" рекламные блоки с помощью специального устройства, вмонтированного в ТВ-приемник или видеомагнитофон). Для телефонной связи более характерен такой вид спама, как хулиганство (включая сходство номеров и ошибки при публикации рекламных объявлений).

Поскольку спам является разновидностью электронной почты, с ним связаны две ключевых составляющих: отправитель и содержимое. Соответственно, нежелательными могут быть как отправители, так и содержимое корреспонденции. Нежелательность содержимого может определить только сам адресат, поэтому акцент в построении защиты надо делать на классификацию отправителей.

Среди отправителей имеются как постоянные ("санкционированные") поставщики входящей корреспонденции (родственники, друзья, коллеги, каналы подписки и т.п.), так и временные ("несанкционированные") поставщики (новые контактные лица, а также… спаммеры).

Итак, для борьбы со спамом нужно:

1) фильтровать входящую корреспонденцию, выделяя в ней санкционированный и несанкционированный потоки;
2) выделять в несанкционированном потоке полезную информацию;
3) вести учет санкционированных и несанкционированных отправителей.

Как же это сделать?

Уроки истории

Давайте вспомним нашу историю [2]. Подобные проблемы весьма эффективно были решены в правительственном аппарате Страны Советов в начале 1930-х годов. К началу Второй мировой

войны и в послевоенный период термины ВЧ и "вертушка", определявшие персональные аппараты высокочастотной правительственной связи, стали привычными и не вызывали вопросов.

Некоторые вехи истории правительственной ВЧ-связи в СССР

Принципы организации высокочастотной связи по проводам обосновал М.В.Шулейкин еще в 1918 г. Практически возможность ВЧ-телефонирования подтвердили П.В.Шмаков и В.А.Куприянов в 1923 г. Спустя 6 лет при одном из отделов ОГПУ было создано отделение правительственной связи. В 1930 г. были сданы в эксплуатацию первые линии ВЧ-связи "Москва-Ленинград" и "Москва-Харьков". В 1936 г. образован отдел связи Главного управления охраны (ГУО) НКВД. С этого момента "вертушка" становится неотъемлемым атрибутом высших чинов Советского государства.

Разделение потоков на "санкционированный" и "несанкционированный" производилось в 1930-е годы с помощью двух телефонных аппаратов: обычного и ВЧ. "Вертушка" обеспечивала фильтрацию звонков по принципу "белого списка" (по нему позвонить могли только доверенные лица). А по обычному телефону фильтрация осуществлялась секретарем (как правило, с использованием "черного списка" нежелательных персон).

Вот теперь можно детально пояснить, как принцип "вертушки" может применяться для борьбы со спамом.

1. Нужно завести два электронных адреса: публичный и приватный ("вертушка").
2. Приватный адрес должен сообщаться только доверенным лицам. Для него должен быть установлен режим фильтрации по "белому списку".
3. Публичный адрес может быть доступен всем. Фильтрация по нему осуществляется традиционными антиспамовыми механизмами (например, теми, что установлены у почтового провайдера), а также по принципу "черного списка".

Это базовая схема. Ее можно совершенствовать разными путями, например, добавив еще один адрес для некоторых отправителей и подписных сервисов (т.е. условно санкционированных отправителей). Что касается исходящей корреспонденции, то если адресат не входит в ваш "белый список", ее нужно отправлять с публичного адреса.

Упомянутая фильтрация легко реализуется как средствами служб бесплатной почты, так и популярными почтовыми клиентами (Outlook, The Bat). Со своими множественными адресами удобно работать путем переадресации всей входящей корреспонденции на единый почтовый ящик, в котором потоки распределяются фильтрами по разным каталогам на основе значения поля адресата (To:) и поля темы (Subject:), т.е. по признаку санкционированности.

Поскольку на публичный адрес будет приходить и полезная корреспонденция, имеет смысл просматривать этот почтовый ящик регулярно (например, раз в неделю), но значительно реже, чем в случае приватного адреса.

Недостатки подхода

"Вертушка" решает проблему выделения доверенных корреспондентов. Но при этом конечно же имеет недостатки.

1. Публичный адрес требуется регулярно просматривать. Это доставляет неудобство тем, кому по роду службы часто приходится сталкиваться с единичными контактами (редакциям СМИ, различным сервисным компаниям и т.п.). На этом уровне необходимо прибегать к традиционным методам борьбы со спамом (маркировке корреспонденции), либо использовать несколько более сложную схему ступенчатой фильтрации.

2. Приватный адрес может подвергаться атакам злоумышленников. Это уже спам из разряда хулиганства. Злоумышленники (либо вредоносные программы) будут "маскироваться" под санкционированный канал за счет подстановки адреса из "белого списка" (напр., при утечке адресов из вашей адресной книги). В этом случае основное внимание надо уделять надежности доверительного канала (в идеале — электронная цифровая подпись корреспонденции; как компромисс — использование условных префиксов в поле Тема (Subject), которые известны отправителю и адресату, а также механизму фильтрации). В силу своей простоты подобные методы априорной маркировки уже применяются разными людьми [3,4]. Условные префиксы-пароли можно применять и для публичного адреса, чтобы отделить новые контакты от спама. Кроме того, можно использовать и метод "серых списков" (greylisting), предложенный Эвансом Харрисом и позволяющим проверять достоверность корреспонденции по трем параметрам: IP-адресу, адресам отправителя и получателя [5].

Автор не разделяет принципов ведения борьбы со спаммерами их же методами, которые порой граничат с хулиганством. Приведенные в статье рекомендации носят защитительный характер и служат простым дополнением к традиционным антиспамовым приемам.

Литература

1. Набережный А., Нартова А. Практический опыт борьбы со спамом и спаммерами // Мир ПК. 2003. №.9–10. http://www.osp.ru/pcworld/2003/09/078.htm
2. В.В. Павлов, В.И. Астрахан, В.Г. Чернега, Б.Г. Чернявский. Правительственная электросвязь в истории России // М., Наука, 2001.
3. Щуров И. Свобода спама или свобода от спама? // Компьютерра. 2002. №41. http://www.computerra.ru/offline/2002/466/21129/
4. Никитин А. Эффективный способ борьбы со спамом // Metamal. 2002. http://www.metamal.com/articles/antispam
5. Харрис Э. New proposal for spam blocking: Greylisting // June 20, 2003. https://www1.ietf.org/mail-archive/working-groups/asrg/current/msg05547.html