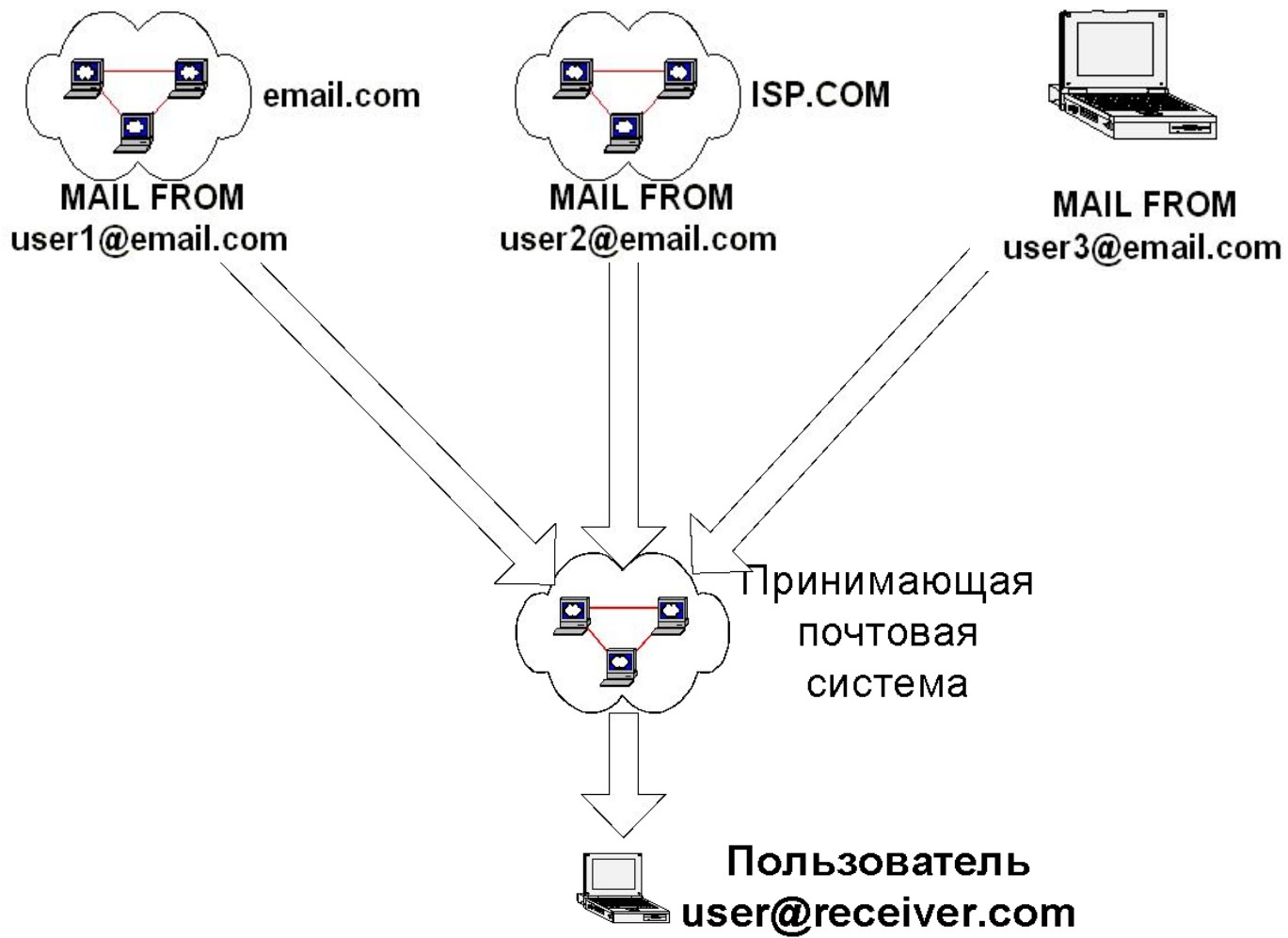

Методы верификации отправителя почтового сообщения

Алексей Тутубалин

lexa@lexa.ru

«Ашманов и Партнеры»



Электронная почта - анонимна

- Любой почтовый сервер может отсылать почту с произвольным адресом отправителя.
 - Классические технологии электронной почты не предоставляют какой-либо возможности верификации.
 - До недавнего времени это считалось приемлемым.
-

Что же изменилось ?

- Возможностью анонимной посылки почты сегодня пользуются:
 - для рассылки спама;
 - для рассылки вирусов;
 - для рассылки мошеннических писем.
- Подавляющее большинство рассылок происходит с компьютеров пользователей («зомби-машины»)
- Как правило, используется поддельный адрес отправителя.
- Обычно в поддельном адресе используется существующий домен.

Постановка задачи

- Если научиться проверять отправителя, то это может отсеять большую долю сегодняшнего спама.
 - Требования к проверке отправителя. Вред должен быть меньше пользы, поэтому:
 - Проверка - дополнительное свойство. Без верификации электронная почта должна продолжать работать.
 - Возможность плавного перехода на новые технологии.
 - Возможность отправки единичного письма незнакомому получателю должна сохраниться.
 - «Нормальные» применения E-mail, включая «автоматических роботов», должны работать.
-

Авторизация SMTP-соединения

- Авторизация «своего» пользователя:
 - использование: корпоративная почта, ISP, почтовые сервисы;
 - не решает проблему входящей извне почты.
 - Авторизация соединения между почтовыми серверами разных организаций:
 - требуется обмен данными авторизации (пароли, ключи)
 - решает проблему только для «постоянных» связей
-

Верификация содержания письма

- Пользователь-пользователь: верификация электронной подписью (S/MIME, PGP-mail):
 - требуется обмен ключами, это задача пользователей.
 - нужна поддержка в клиентских программах
 - ради разового обмена почтой никто не будет меняться ключами.
- Сервер-сервер: Yahoo Domain Keys
 - публикация ключей и политики их использования в DNS
 - требуется модификация почтовых серверов как для простановки подписи, так и для её верификации.

Авторизация по IP-адресу отправителя

- На основании уже существующих данных (reverse resolving в DNS):
 - Не требует изменения инфраструктуры, уже широко применяется.
 - Отсутствие достоверных данных о структуре чужих сетей ограничивает применимость.
 - Новые методы
 - дополнительные данные в обратной DNS-зоне (MTA Mark, Selective Sender, MX Out)
 - дополнительные данные в DNS домена отправителя (SPF Classic, CallerID, SenderID, RMX)
-

Yahoo Domain Keys

- **Идея метода:**
 - публикация в DNS публичного ключа домена
 - текст и заголовки сообщения подписываются
 - на приемной стороне подпись проверяется
 - **Достоинства**
 - «достоверность» является свойством письма, а не почтовой сессии
 - **Недостатки**
 - при внедрении на публичном сервисе, можно получить любое нужное количество подписанных сообщений.
-

YDK: технические детали

Пример записи в DNS:

```
beta._domainkey.gmail.com      text = "t=y;  
k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4..."
```

Заголовки в письме:

```
DomainKey-Signature: a=rsa-sha1; c=noaws;  
s=beta; d=gmail.com;  
h=received:message-id:date:from...  
b=Gjon40A2c8NfLCBauZskv99Eks....
```

YDK: перспективы

- Подход перспективный, но есть проблемы:
 - при поддержке YDK на публичном сервисе можно получить любое количество подписанных сообщений.
 - Неясно что делать, если требуется изменить один из подписанных заголовков (например, Resent-From при пересылке).
 - Пропуск подписанных писем мимо фильтра породит злоупотребления, нужен отдельный рейтинговый сервис.

SPF Classic

1. Владелец домена публикует в DNS «политику» - список IP-адресов с которых может исходить почта данного домена:

```
"v=spf1 +ip:192.168.0.0/16 +mx ?all"
```

Каждый элемент списка состоит из префикса и диапазона IP-адресов. Возможны такие префиксы:

- ❑ + **pass** - разрешающий префикс. +all почта «из данного домена» может приходиться с любого адреса
 - ❑ - **fail** - запрещающий префикс. –ip:10.0.0.0/8 – почта не может приходиться с этого адреса.
 - ❑ ~ **softfail** «нейтрально-отрицательный» префикс. «Адрес может не быть разрешенным».
 - ❑ ? **neutral** «нейтральный» - владелец адреса не может ничего сказать про данный IP.
2. В ходе SMTP-сессии реальный IP-адрес посылающей стороны сравнивается со списком от владельца домена, после чего принимается решение о статусе письма.

SPF: проблема пересылок

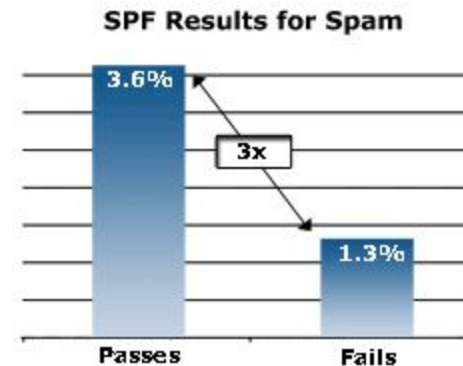
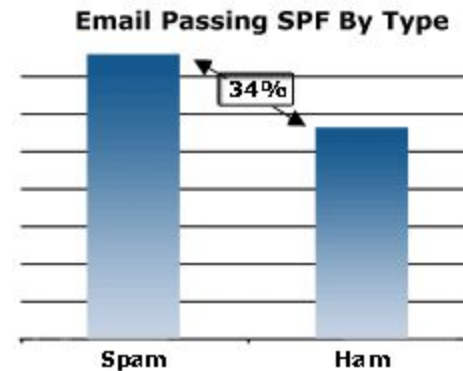
- Неустранимое противоречие
 - «Мягкая» политика не помогает от фальсификации адресов
 - Жесткая политика приводит к потерям при пересылках (forward) писем: в процессе пересылки адрес отправителя сохраняется, а IP-адрес посылающей стороны – нет.
- Для внедрения жестких SPF-политик требуется модификация ПО на почтовых серверах «третьих сторон».

SPF Classic: прочие проблемы

- Массовая PR-компания породила массовое внедрение со множеством ошибок.
 - «Политики по-умолчанию». Уровень поддержки технологии невысок, поэтому существующие реализации технологии позволяют «придумать» политику домена если ее нет.
 - Потенциально-опасный механизм «exists» - отправитель письма может следить за его путем по вашей сети.
 - Спамеры уверенно осваивают SPF.
-

SPF и спам

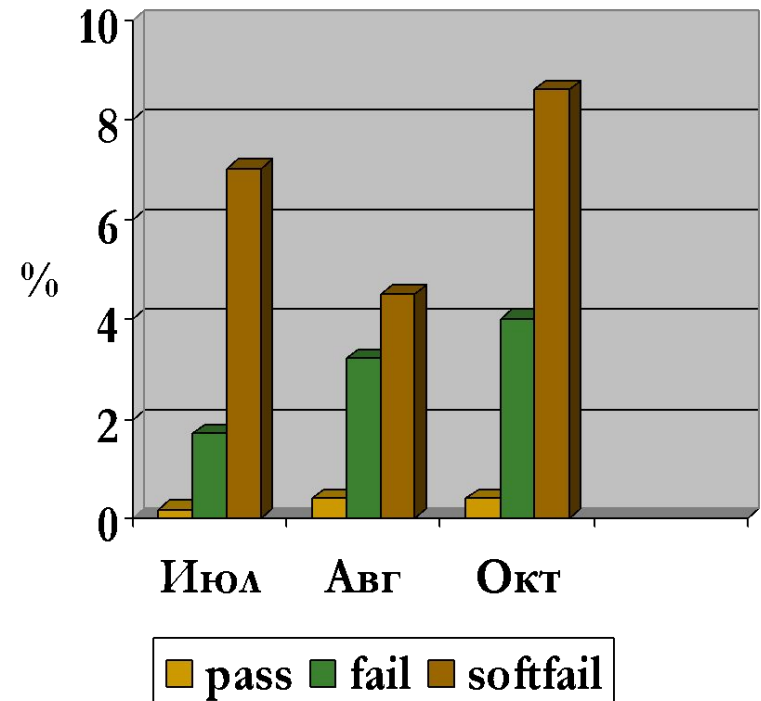
- По данным CipherTrust, спамеры освоили SPF быстрее «нормальных» систем.
- Распространенность SPF на сегодня недостаточна, чтобы быть эффективным антиспам - средством.



SPF как фильтр спама

- Статус fail (неверный отправитель) получают <4% спам -писем.
- Статус pass – 0.4%
- Статус softfail (владелец домена не уверен) – 5-8% спама и около 1% нормальной почты.
- Уровень поддержки технологии вырос с 8% в июле до 13% в октябре.

SPF-статусы для спам-почты



SPF как источник дополнительных данных для антиспам - фильтра

Для фильтра SpamTest на большом потоке сообщений:

- примерно для 0.5% сообщений статус SPF более «жесткий», чем результат работы Spamttest.
- Примерно для 0.4% сообщений, статус более «мягкий» (доля совпадает с долей «pass» в потоке спама).

Вывод: польза от SPF сомнительна.

SPF: рекомендации

- Публикация SPF-политики полезна, во всяком случае ее не будут придумывать за вас.
 - публикация «жесткой» политики будет приводить к потерям исходящей почты
 - публикация «мягкой» политики может привести к ее игнорированию получателями
 - Нужен нейтральный вариант, например:
`+ip:10.0.0.0/24 ~all`
`+ip:192.168.0.0/24 ?all`

SPF: рекомендации (2)

1. При приеме почты нельзя принимать решение только на основании SPF
 2. Если первое условие соблюдено, то SPF может быть полезным источником данных для антиспам-системы.
 3. К несчастью, основные публично-доступные реализации SPF не удовлетворяют условию 1 (исключение: SpamAssassin)
-

CallerID, SenderID

- CallerID – технология Microsoft с похожими на SPF идеями.
 - SenderID – объединение SPF Classic и CallerID:
 - Базовые идеи от SPF
 - Синтаксис от CallerID
 - Методика определения адреса отправителя – от CallerID
 - SenderID не был поддержан IETF и сообществом OpenSource, перспективы туманны.
-

Выводы

1. Ожидать кардинального технического решения проблемы подделки отправителя не стоит.
 2. Частные решения возможны, например YDK может быть интересна сервисам легальных массовых рассылок.
 3. Спамеры быстро адаптируются к новым технологиям, а все предлагаемые меры не содержат защиты от этого.
 4. Верифицировав отправителя, ничего сказать о самом сообщении все равно нельзя. Решением может быть наложенный рейтинговый сервис.
-

Спасибо за внимание

Пожалуйста, задавайте вопросы.
