Técnicas Anti-Spam no NIC.br

Paulo Bernardo Severiano da Silva - pbsilva@nic.br
Operações - NIC.br
Eduardo Sztokbant - eduardo@registro.br
Engenharia – Registro.br

Conteúdo

- Motivação/Objetivo
- Mecanismo: Fluxograma das mensagens
- Técnicas adotadas: particularidades e problemas
  - SPF – Sender Policy Framework.
  - Greylisting
  - Amavisd-new
  - Clamav
  - Spamassassin
- Conclusão

Motivação

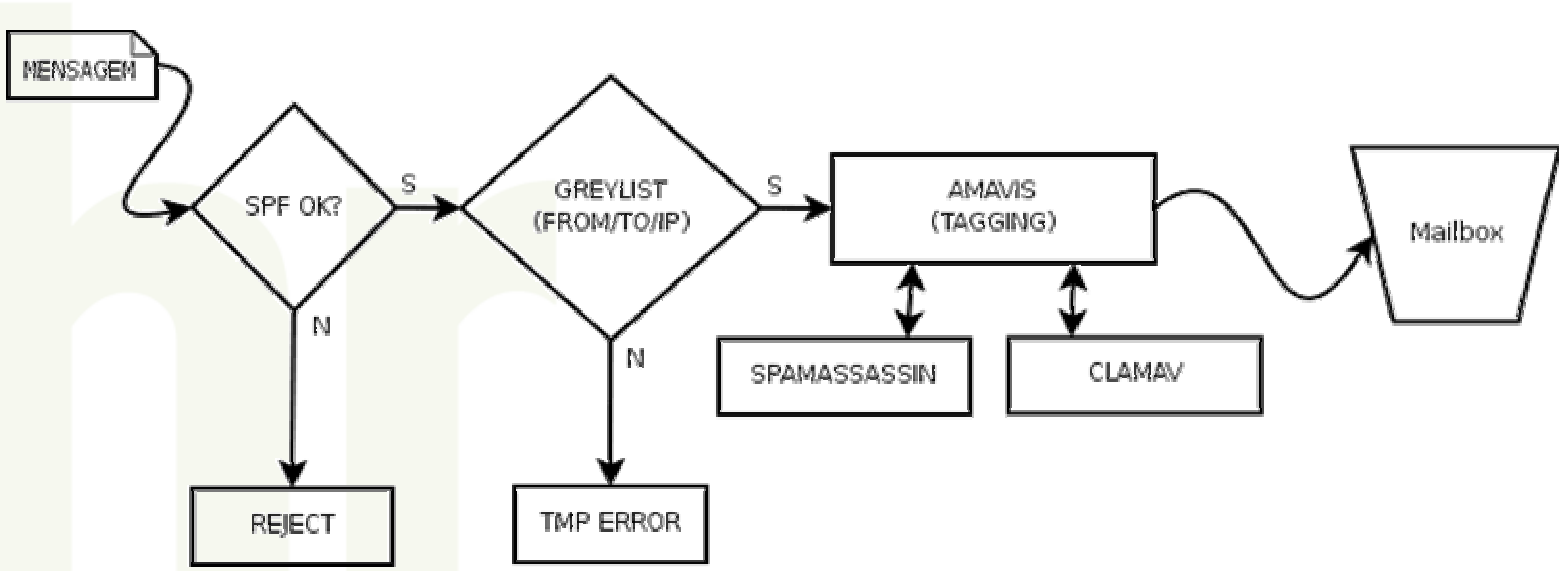
- Motivação:
  - Até março deste ano, cerca de 86% de todos os e-mails trocados na Internet são SPAMS *(*fonte: Eletronic Commerce in Canada[1]*)*
    [1] *http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/Intro*
  - Mensagens indesejadas diminuem a produtividade e aumentam custos.
  - O uso exclusivo de filtro bayesiano (Bogofilter) não estava mais sendo suficiente.

Objetivo

- Diminuir ao máximo o número de mensagens não-solicitadas na rede do NIC.br.

- Princípios
  - Minimizar o impacto para o usuário.
  - Não perder mensagens legítimas.
  - Utilização de ferramentas livres!!

Mecanismo


MENSAGEM
SPF OK?
S
N
GREYLIST
(FROM/TO/IP)
S
N
AMAVIS
(TAGGING)
SPAMASSASSIN
CLAMAV
Mailbox
REJECT
TMP ERROR

SPF – Sender Policy Framework

- **Funcionamento:**
  - Depende de duas partes distintas e independentes

    1) Publicação no DNS das máquinas autorizadas a enviar e-mails @domínio

    ```
    registro.br. IN TXT  "v=spf1 a mx a:mailexploder.registro.br -all"
    ```

    2) Verificação do record DNS publicado feita pelo servidor recipiente

  - Os mecanismos são avaliados sequencialmente e podem ser prefixados por:

    - fail **~** softfail

    + pass **?** neutral
  - Default: pass

SPF – Sender Policy Framework

- **Particularidades**

  - O sucesso do SPF é proporcional à sua adoção pela comunidade, tanto na verificação quanto na publicação dos records.

  - Muitos dos grandes servidores publicam records TXT relativos ao SPF (ex: UOL, Terra, Gmail, Hotmail...)

SPF – Sender Policy Framework

- **Problemas enfrentados**

  - Usuários que usam mais de uma conta de e-mail e enviam suas mensagens por apenas um servidor.
    ➔ solução: estudar atentamente todas as máquinas a serem incluídas no record SPF.

  - Verificação de SPF após forward interno da mensagem: aparentemente a mensagem terá vindo de um servidor interno, provavelmente inválido.
    ➔ solução: SPF deve ser configurado no MTA da borda.

Greylisting

Funcionamento:

Princípio: MTAs legítimos funcionam conforme a RFC 2821, fazendo tentativa de reenvio ao receber um erro temporário, diferentemente de spammers e vírus na maioria das vezes.

Baseia-se na trinca From, To e IP de origem da mensagem.

Mensagens com trincas jamais vistas antes, recebem erro temporário.

Se há nova tentativa após um delay pré-determinado (normalmente 5 minutos) a mensagem é aceita.

Greylisting

Particularidades:

- Possibilidade de coordenar com whitelists

Problemas enfrentados:

- Transtorno para usuários que não querem ou não podem esperar reenvio da mensagem.
- Alguns MTAs legítimos não retransmitem a mensagem ao receber um erro temporário. Estes devem ser colocados em whitelist.

Amavisd-new

- **Funcionamento:**
  - Interface entre o MTA e controladores de conteúdo
    - Spamassassin: classificação de ´Spamicidade´
    - Clamav: verificação de vírus
- **Particularidades:**
  - Mensagens nunca são rejeitadas, apenas “etiquetadas” para que os usuários não percam mensagens classificadas erroneamente.
- **Problemas enfrentados:**
  - Atenção ao espaço em disco X mensagens em quarentena

Spamassassin/Clamav

- **Utilização**
  - Somente tagging, mensagens serão entregues de qualquer maneira
- **Spamassassin**
  - Diversos mecanismos de classificação, inclusive bayesiana
  - Problema encontrado: reclassificação de falsos-positivos e falsos-negativos
- **Clamav**
  - Acrescenta *warning* às mensagens infectadas
  - Verifica dentro de arquivos compactados

Conclusão

- Resultados excelentes, imediatamente notados e elogiados pelos usuários.
- Flexibilidade de *whitelists* permitiu um ótimo aproveitamento dos benefícios do SPF e Greylisting.
- Atualmente é praticamente inviável a não implementação de políticas anti-spam.
- A combinação de múltiplas etapas se mostrou extremamente eficiente, pois uma acaba suprindo a deficiência da outra. Na prática a esmagadora maioria das mensagens que passou pelos filtros (SPF/Greylisting) acabou sendo classificada corretamente pelo SpamAssassin.

Links relacionados

- Amavisd-new http://www.ijs.si/software/amavisd/
- Spamassassin http://spamassassin.apache.org/
- Clamav http://www.clamav.net/
- SPF http://spf.pobox.com/
- Greylisting http://www.greylisting.org/

- Registro.br http://registro.br

Perguntas

?

Paulo Bernardo Severiano da Silva - pbsilva@nic.br
Operações - NIC.br
Eduardo Sztokbant - eduardo@registro.br
Engenharia – Registro.br