Spam e fraudes

Técnicas de mitigação para administradores de redes

baseado em http://antispam.br/admin/

Agenda

Conceitos Fundamentais

* A Estrutura da Mensagem
* O Funcionamento do Correio Eletrônico
* Algumas Técnicas de Envio de Spam que devem ser combatidas

Técnicas para Redução do spam recebido

* Listas de Bloqueio
* Filtros de Conteúdo
* Greylisting

Técnicas para Combater a Falsificação de Endereços

* SPF
* DKIM

Boas Práticas de Configuração para Evitar o Abuso da Rede

Conceitos Fundamentais

A Estrutura da Mensagem (RFC2822)

Envelope

Informações para o MSA ou MTA saiba o que fazer com a mensagem
Existem somente durante a transmissão da mensagem.

```
mail from: <danton.nunes@inexo.com.br>
rcpt to: <jessen@cert.br>
rcpt to: <ethy.brito@inexo.com.br>
```

em caso de erro

entrega normal

Cabeçalho

Campos com dados úteis tanto para servidores quanto aplicativos.
Fazem parte da mensagem.

```
Return-path: <danton.nunes@inexo.com.br>
From: Danton Nunes <danton@cert.br>
To: Klaus <jessen@cert.br>
Cc: Ethy H. Brito <ethy.brito@inexo.com.br>
Subject: Slides para SSI/2006
```

A Estrutura da Mensagem

Cabeçalho (cont.)

Campos mais importantes no gerenciamento de problemas relativos a spam

Return–Path: geralmente copiado do envelope (MAIL FROM), é o endereço para onde vão mensagens de erro. Pode ser vazio!

Received: indica a procedência (pelo endereço IP), a data e a hora em que a mensagem foi recebida.
Analisando os vários Received: é possível recuperar o caminho que a mensagem percorreu, mas ATENÇÃO: somente o Received: mais recente é digno de confiança, os demais podem ser falsos!

From: designa o remetente nominal da mensagem, que não é necessaria–mente igual ao que aparece no envelope ou no campo Return–Path:.

To: Cc: Bcc: designam os destinatários que não necessariamente coinci–dem com os declarados no envelope.
Bcc: é deletado antes da entrega da mensagem.

A Estrutura da Mensagem

Corpo da mensagem

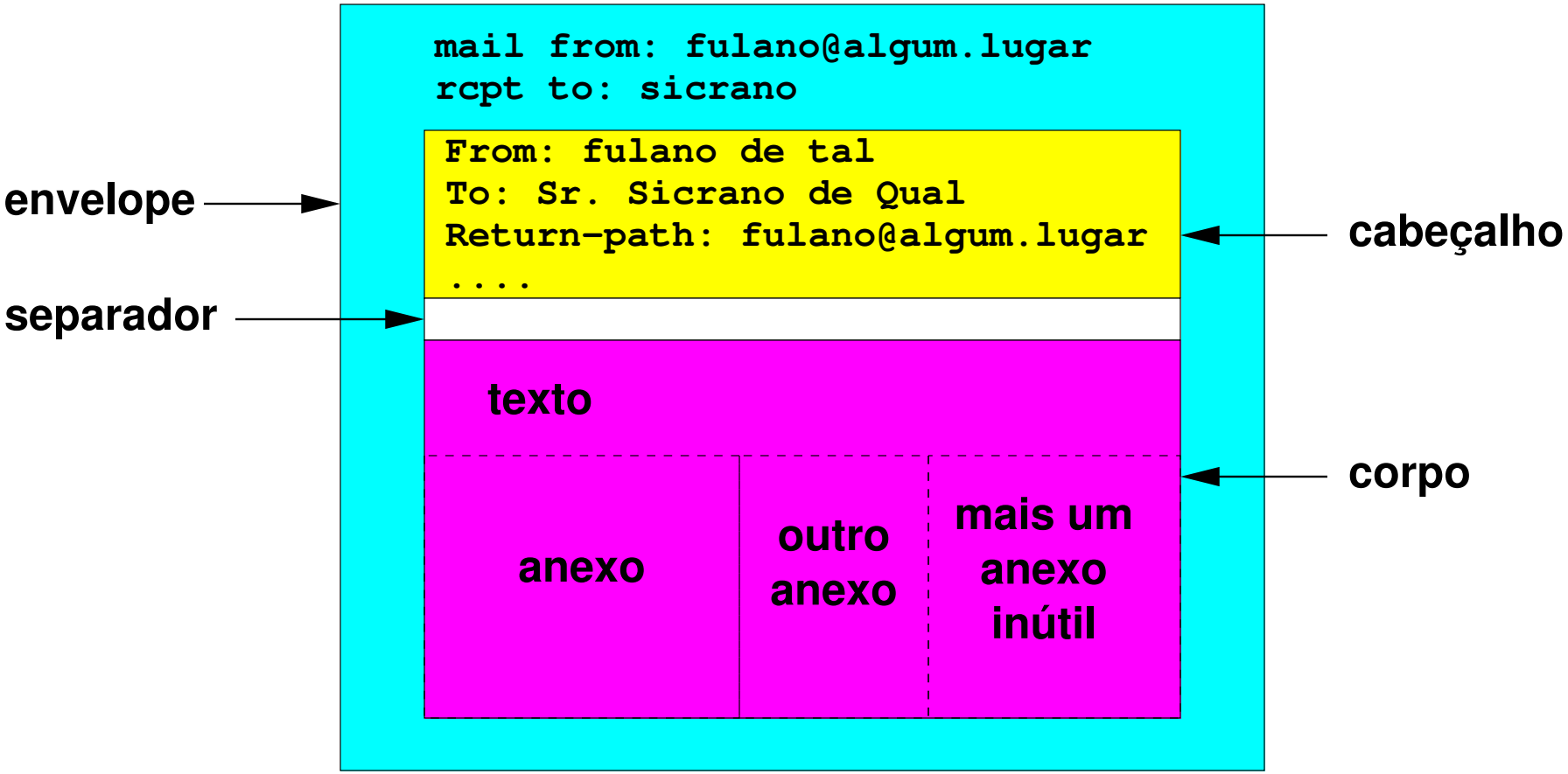
O corpo da mensagem contém seu texto e anexos, se houverem. O formato e a codificação do corpo são descritos pelos campos Content–type: e Content–Transfer–Encoding: e, em caso de mensagens complexas, MIME–Type:.

O corpo da mensagem é separado do cabeçalho por uma linha em branco.

MTAs não lidam com o corpo da mensagem. Alguns programas auxiliares de MTAs, entretanto, podem processar o corpo das mensagens, tais como anti–vírus e anti–spam baseados em análise de conteúdo.

A Estrutura da Mensagem

Resumindo



O Funcionamento do Correio Eletrônico

Conceitos

*** Caixa postal:** é um arquivo ou diretório onde as mensagens são recebidas.

*** MUA (Mail User Agent):** é uma aplicação ou programa utilizado diretamente pelo usuário para compor, enviar e ler mensagens. Exemplos de MUAs são: Pine, Mutt, Mozilla Thunderbird, etc.

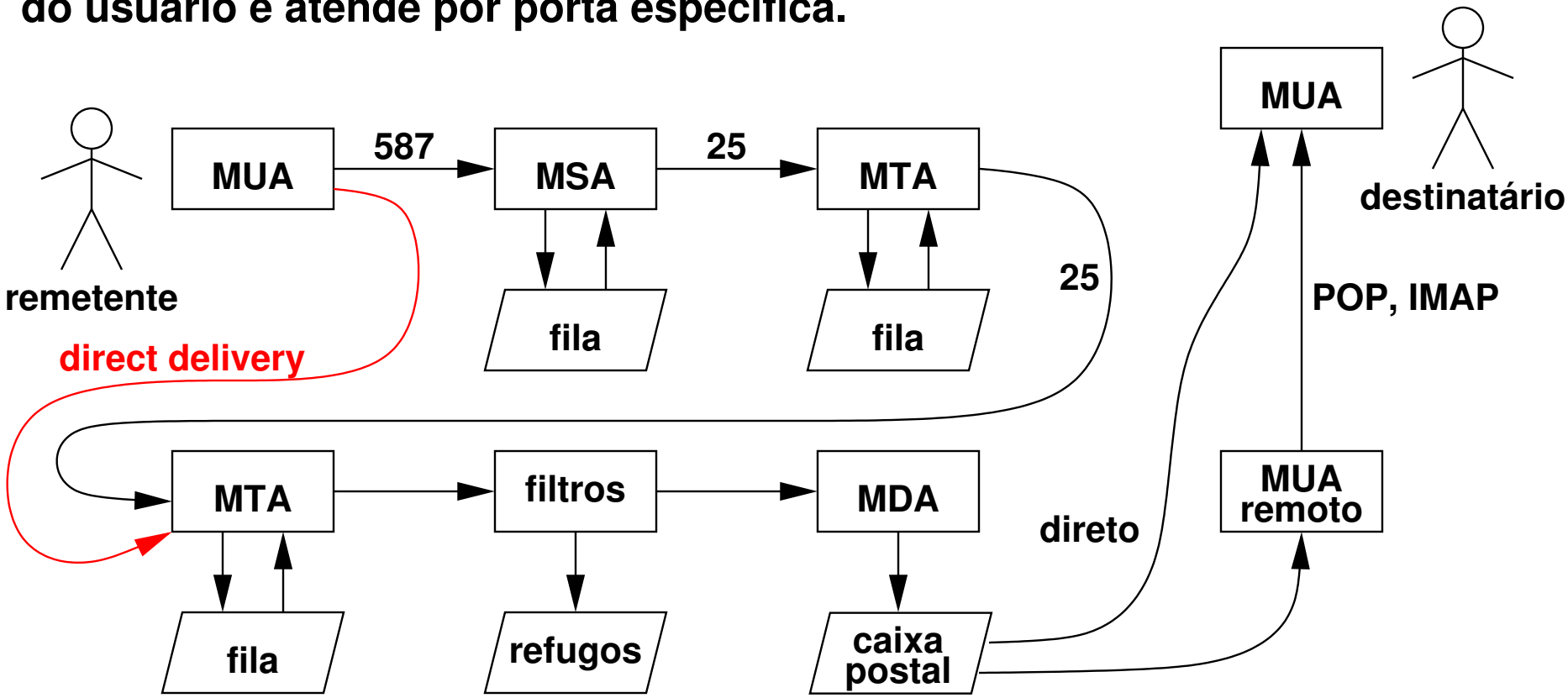
*** MDA (Mail Delivery Agent):** é uma aplicação responsável por entregar mensagens em caixas postais. Um exemplo de MDA é o Procmail.

*** MTA (Mail Tranfer Agent):** é uma aplicação responsável por passar mensagens para outros MTAs ou para um MDA, se o destino da mensagem for respectivamente remoto ou local. Há vários MTAs, por exemplo: Sendmail, Qmail, Exim e Postfix.

O Funcionamento do Correio Eletrônico

Conceitos

*** MSA (Mail Submission Agent): é como o MTA, mas requer autenticação do usuário e atende por porta específica.**



Um dia na vida de uma mensagem

Algumas Técnicas de Envio de Spam

» **programas de envio de e–mail em massa**

Estes programas são fáceis de obter e podem ser configurados para enviar e–mails através de máquinas com proxies abertos.

» **spam zombies**

são computadores de usuários finais que foram comprometidos por códigos maliciosos em geral, como worms, bots, vírus e cavalos de tróia. Estes códigos maliciosos, uma vez instalados, permitem que spammers utilizem a máquina para o envio de spam, sem o conhecimento do usuário.

» **vírus propagados por e–mail**

normalmente são recebidos como um arquivo anexado à uma mensagem de correio eletrônico. O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, executando o vírus, que infecta arquivos e programas e envia cópias de si mesmo para os contatos encontrados nas listas de endereços de e–mail.

Algumas Técnicas de Envio de Spam

» **abuso de formulários e scripts na Web**

muitos serviços Web tem algum tipo de transmissão do conteúdo de formulários por e–mail, sendo que tal funcionalidade pode ser abusada para a transmissão de spam.
Um exemplo de funcionalidade que pode ser abusada é a função mail() da linguagem PHP e seus similares em outras linguagens.
Spams enviados a partir de servidores Web mal–configurados são dificilmente contidos pelas práticas atuais de contenção.

» **uso de sites comprometidos**

servidores comprometidos ou conquistados por crackers estão entre as plataformas de lançamento preferidas do spammer. Sua identidade é preservada e quando o esquema é eventualmente descoberto, quem se compromete é o administrador do sistema invadido.

Algumas Técnicas de Envio de Spam

Exemplo: abuso de formulários e scripts na Web

O alvo são formulários que enviam e–mail, através de scripts mal escritos ou "ingênuos".

Métodos em PHP e linguagens similares que enviam e–mail não fazem crítica dos dados que recebem, o que permite que sejam subvertidos para enviar e–mail para destinatários não planejados.

Spam enviado por meio de formulários é praticamente invencível pois:

- **» vem de um servidor válido => engana SPF e greylisting;**
- **» vem de remetente válido e pode ser assinado => engana DKIM;**
- **» o perpetrante fica completamente anônimo.**

Como resolver? Escrever os programas de web defensivamente!

Algumas Técnicas de Envio de Spam

Exemplo: abuso de formulários e scripts na Web

```
<form action="send.php" method="post">
 <p><label for="from">Seu e-mail, para resposta</label>
  <input type="text" name="from" size="40" /></p>
 <p><label for="msg">Entre a sua mensagem</label>
  <textarea cols="40" rows="8" name="msg"></textarea></p>
 <input type="submit" value="Enviar"
    onclick="return validate(this.form)" />
</form>
```

A função "validate" retorna 0 nos seguintes casos:
1. "from" não contém um endereço de e–mail válido;
2. a mensagem está vazia.

Algumas Técnicas de Envio de Spam

Exemplo: abuso de formulários e scripts na Web

Seu e–mail para resposta

danton.nunes@inexo.com.br

Entre a sua mensagem

Querido Papai Noel,
Neste ano eu fui bonzinho, fiz toda a lição de casa, então eu acho que mereço um presente bem legal. Neste Natal eu quero um Mac mini com Intel Dual Core rodando a última versão do MacOS-X.
obrigado!

Enviar

Algumas Técnicas de Envio de Spam

Exemplo: abuso de formulários e scripts na Web

send.php

```
<script language="php">
  if (mail('faleconosco@exemplo.com.br',
        'mensagem recebida pelo formulário',
        $_POST['msg'],
        'From: '.$_POST['from'])) success();
  else failure();
</script>
```

Parece bom, afinal os dados em $_POST já foram verificados antes de serem enviados. Pois é, PARECE bom, mas não é.

Há dois pressupostos falsos aqui que permitem exploração.

Algumas Técnicas de Envio de Spam

Exemplo: abuso de formulários e scripts na Web

Pressupostos falsos:

1. O cliente vai executar a função 'validate' que garante que só dados válidos serão submetidos;

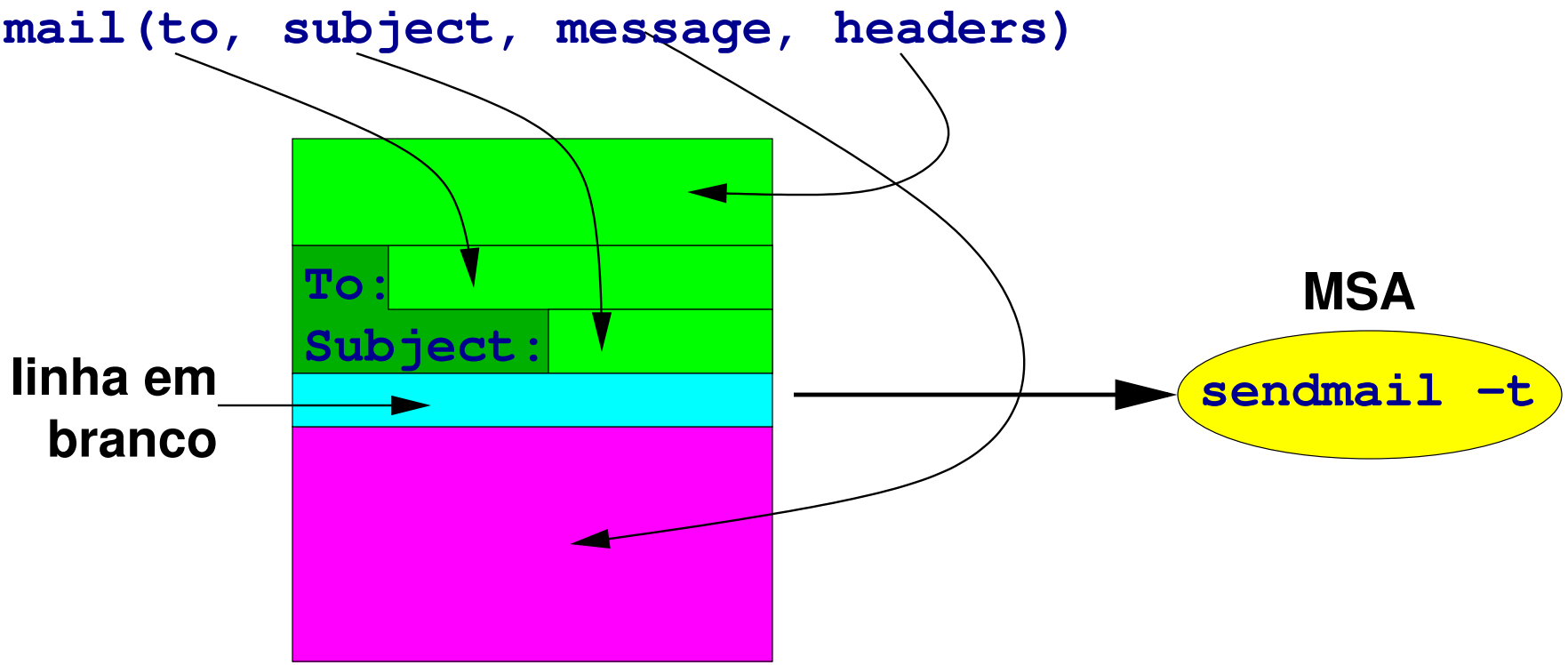
2. A função 'mail' do PHP faz o que promete, isto é, envia uma mensagem para o endereço que está no primeiro argumento.

E está armado o caminho para o desastre.

Algumas Técnicas de Envio de Spam

Exemplo: abuso de formulários e scripts na Web

Função 'mail' do PHP (e de tantas outras linguagens)



Algumas Técnicas de Envio de Spam

Exemplo: abuso de formulários e scripts na Web

```
telnet www.exemplo.com.br 80
POST send.php HTTP/1.0
host: www.exemplo.com.br
Content-type: text/plain
Content-length: 3546

from=J. D. Spammer <jd@spammers.r.us>
Bcc: Pato1 <huguinho@disney.com>
Bcc: Pato2 <zezinho@disney.com>
Bcc: Pato3 <patolino@warner.bros.com>

Caro Pato,

Você foi indicado por um amigo para participar desta promoção
especial bla bla bla, basta clicar aqui, quac quac quac....
```

tudo isto vai parar em $_POST['from']

linha em branco, separando cabeçalho do "corpo" da mensagem

spammers adoram Bcc:!

isso, clica, clica!

Algumas Técnicas de Envio de Spam

Exemplo: abuso de formulários e scripts na Web

Resultado do ataque:

- » A mensagem vai para os "patos" indicados nos Bcc:
- » O usuário real do formulário nem fica sabendo!
- » Envio por meio de MSA/MTAs perfeitamente válidos.

Solução:

- » Programação defensiva, isto é, validar os dados recebidos por formulário do lado servidor, mesmo que isso tenha sido supostamente feito no lado cliente.

Mas nem tudo está perdido:

- » A maioria dos servidores Web rodam sob usuários conhecidos (www, nobody, apache, etc.), portanto é possível estabelecer uma regra de filtragem com essa base.

Técnicas para redução do spam recebido

São políticas aplicadas na recepção das mensagens, envolvendo MTA de recepção, MDA (entrega) e MUA (ferramenta do usuário)

Miram diferentes características do spam: origem, forma, conteúdo, comportamento.

Principais técnicas

- Listas de bloqueio (e de exceção)
- Filtros de conteúdo
- Greylisting

O uso destas técnicas implica em algum esforço por parte de quem recebe o spam. Nenhuma é infalível, muito pelo contrário...

Listas de bloqueio

Introdução

Listas de bloqueio são, talvez, o mais antigo mecanismo de combate ao spam. Estas listas são bases de dados de endereços IP que tenham sido identificados como possível fonte de spam, segundo os critérios da entidade que mantém a lista. As listas normalmente funcionam através de consultas DNS às bases de dados.

Também existem outros critérios de bloqueio, geralmente envolvendo DNS, como:

* bloqueio pela inexistência de reverso;
* bloqueio pela inconsistência do reverso;
* bloqueio pela presença do reverso em uma lista negra de domínios.

Listas de bloqueio

Listas negras

As listas negras (blacklists) possuem endereços IP de máquinas que, segundo o critério do mantenedor da lista, estão envolvidos em envio de spam.

Estas listas são implementadas através de zonas de DNS, semelhantes às de tradução reversa. Dado um endereço IP w.x.y.z a ser bloqueado, na lista este IP será incluído com o nome de domínio z.y.x.w.nome.da.lista.

Se ao consultar uma lista negra pelo nome z.y.x.w.nome.da.lista for obtida uma resposta, significa que o IP w.x.y.z faz parte da lista negra. A resposta obtida costuma indicar a razão pela qual o IP foi incluído na lista de bloqueio, e varia de lista para lista.

Listas de bloqueio

Listas negras (cont.)

A implementação de consultas a listas negras é bastante fácil e praticamente todo MTA possui suporte para este recurso.

É importante ter muito cuidado ao escolher quais listas consultar. Algumas listas possuem critérios de inclusão de IPs pouco seletivos, pois em geral incluem grandes blocos de rede, podendo incluir na lista de bloqueio muitos IPs que não estão envolvidos em spam. Algumas chegam a incluir todos os IPs de um determinado país, por exemplo.

Para evitar o bloqueio de e–mails legítimos, que venham de redes apenas vizinhas de IPs que enviam spam, é aconselhável a utilização de listas que tenham um bom critério de inclusão de IPs. Um documento de referência para a escolha das listas é o relatório do San Diego Supercomputing Center, *http://www.sdsc.edu/~jeff/spam/Blacklists_Compared.html.*

Listas de bloqueio

Listas negras (cont.)

Também é possível criar uma lista negra própria, desde que se tenha acesso a um servidor de nomes, e nele listar os endereços IP que violem alguma política pré–estabelecida.

Cuidados

O maior problema com listas negras são os falsos positivos, isto é, endereços que estão listados apenas por pertencerem a determinados blocos "malditos". => O inocente paga pelo culpado.

Acontece freqüentemente de um conjunto de IPs permanecer listado muito tempo depois de o problema que o levou à lista ter sido sanado.

Use listas negras como um último recurso, apenas para mensagens que não foram aprovadas (ou rejeitadas) por outros critérios.

Listas de linhas discadas

São listas que enumeram os domínios reversos de redes dedicadas somente ao acesso doméstico, seja propriamente discado ou de banda larga.

O funcionamento é semelhante às listas negras, mas neste caso o domínio consultado é o reverso clássico (in–addr.arpa). Se o domínio resultante for sub–domínio de qualquer um listado, a mensagem é rejeitada.

Cuidado: Vários operadores de ADSL não fazem separação de seus usuários domésticos dos corporativos.

Listas de bloqueio

Listas de relays e proxies abertos

Relays abertos são MTAs que transmitem mensagens de qualquer domínio, ou mesmo só de domínios determinados, para qualquer outro, sem pedir autenticação, sem restringir (ou restringindo muito pouco) a faixa de endereços IP de origem. Relays abertos podem ser MTAs mal configurados ou programas instalados clandestinamente em máquinas comprometidas.

Proxies abertos usam um mecanismo diferente, mas com o mesmo efeito. Em vez de um MTA ser abusado, é um serviço de proxy que é abusado para retransmitir mensagens, por exemplo, através do comando CONNECT.

As listas de relays e proxies abertos funcionam exatamente como as listas negras convencionais. Algumas listas negras mais gerais retornam valores indicativos de que o IP foi incluído lá por ser um relay ou proxy aberto.

Listas de bloqueio

Lista branca (ou de exceção)

A lista branca (whitelist) consiste em uma lista de exceções às regras de bloqueio por listas negras ou outros critérios. Normalmente a lista branca é mantida pelo próprio administrador do serviço de e–mail, e pode ser implementada através de DNS, listas de domínios, IPs ou blocos CIDR, ou através de regras de SPF que devem ser avaliadas antes de qualquer outra.

Por exemplo, usando SPF, se quiséssemos que qualquer IP da rede 192.0.2.0/24 pudesse enviar mensagens independentemente de registros SPF (ou a falta deles), ou mesmo que constem de alguma lista negra, bastaria incluir um registro SPF contendo ip4:192.0.2.0/24 para colocá–lo na lista branca.

Listas de bloqueio

Checagem de informações de DNS e de aderência a RFCs

Um método de bloqueio utilizado por alguns administradores de redes é impedir o recebimento de mensagens partindo de máquinas cujo endereço IP não possui um registro DNS do tipo PTR (endereço reverso). Adicionalmente também é possível verificar se o nome da máquina, retornado pela consulta PTR, possui um registro do tipo A que seja igual ao endereço IP originalmente consultado.

Normalmente o bloqueio em função do endereço reverso está associado com algum outro critério, como por exemplo, determinar se o transmissor é um provável usuário doméstico, de linha discada, ADSL ou cabo, uma vez que estas máquinas não são MTAs e muitas vezes podem ser spam zombies.

Listas de bloqueio

Checagem de informações de DNS e de aderência a RFCs (cont.)

Há duas considerações que devem ser feitas sobre o bloqueio em função do endereço reverso de máquinas de usuários domésticos:

* este depende de convenções adotadas pelo provedor de serviços da rede de origem. Estas convenções podem mudar sem aviso prévio e não são uniformes entre diversos provedores;

* pode fazer com que MTAs válidos sejam bloqueados.

Cuidado: possuir endereço reverso não é obrigatório, além disso, nem sempre os administradores de redes possuem controle direto sobre a configuração DNS de seus IPs. Desse modo, bloqueio em função do endereço reverso deve ser usado com cautela.

Listas de bloqueio

Considerações finais sobre listas de bloqueio

É importante sempre lembrar que, ao utilizar listas de bloqueio, existe o risco de mensagens legítimas serem bloqueadas. Existem outras técnicas, como SPF e greylisting, que não se baseiam somente em informações sobre o IP que está enviando o e–mail e possuem uma taxa menor de falsos positivos.

RESUMINDO:

Só use se tudo mais falhar!

Filtros de conteúdo

Introdução

Existem algumas técnicas de bloqueio de spam que se baseiam na análise do conteúdo da mensagem, reconhecendo padrões do conteúdo que buscam identificar se o e–mail pode conter um vírus ou se tem características comuns aos spams.

Tais filtros podem ser usados em conjunto com o MTA, MDA, ou ainda no aplicativo do usuário.

Uma vez que uma mensagem foi reconhecida como possivelmente hostil, ela pode ser:

Rejeitada com erro 550 5.7.1. Message content rejected	aceita, porém desviada para quarentena	aceita e enviada para destinatário com marca de "suspeita"

Filtros de conteúdo

Anti–vírus

Existem no mercado diversas opções de anti–vírus que podem ser utilizados em conjunto com MTAs, sendo que algumas destas opções são gratuitas. A maioria possui mecanismos de atualização automática, já que a criação de novos vírus é bastante intensa e exige atualizações diárias, ou até mesmo mais freqüentes, das assinaturas dos anti–vírus.

Os programas anti–vírus não lidam diretamente com arquivos comprimidos ou no formato usual dos e–mails. Deste modo, antes do conteúdo da mensagem ser analisado pelo anti–vírus é necessário desmontar a mensagem e possivelmente descomprimir os anexos. Um programa muito comum para realizar estas tarefas é o Amavis.

Devido ao trabalho de desmontagem da mensagem e depois o de reconhecimento de padrões, o uso de anti–vírus em conjunto com MTAs costuma implicar em altos consumos de CPU e memória do servidor. Deste modo, aconselha–se submeter as mensagens ao anti–vírus somente depois de terem sido avaliadas por outras técnicas.

Filtros de conteúdo

Filtros Bayesianos anti–spam

Analisam o conteúdo da mensagem e avaliam a probabilidade dela ser spam em função de uma base de conhecimento pré armazenada.

É necessário treinar o filtro, para que ele forme a base de dados, injetando mensagens boas e ruins. O treinamento pode ser contínuo e concomitante com a operação regular

Um filtro bastante popular de reconhecimento de spam é o SpamAssassin, um script em Perl.

Os mesmos programas usados para desmontar mensagens para anti–vírus podem acionar filtros anti–spam. Ao contrário dos anti–vírus, porém, o foco desses filtros é muito mais o texto da mensagem do que os anexos.

Filtros de conteúdo

Filtros Bayesianos anti–spam (cont.)

O consumo de recursos computacionais é elevado, porém menos crítico que no caso dos anti–vírus, mas mesmo assim pode ser comprometedor em servidores de alto tráfego.

Para que o filtro se adapte ao caráter mutável do spam é necessário que o treinamento do filtro seja contínuo, com a identificação dos spams que não foram classificados e das mensagens que não são spam e que foram rotuladas como tal.

Como os filtros Bayesianos podem acarretar falsos positivos, é aconselhável não descartar uma mensagem marcada como spam, mas sim optar por colocá–la em quarentena. Esse problema pode ser agravado caso a base de dados com que ele toma decisão for desatualizada ou baseada em outro idioma.

Filtros de conteúdo

Filtros Bayesianos anti–spam (cont.)

Outra questão a ser considerada é o fato de estes filtros poderem ser driblados por spammers que introduzam "ruídos" em suas mensagens, ou seja, além do texto do spam são também introduzidas palavras aleatórias, letras, palavras em outros idiomas, etc. Deste modo, a análise estatística das ocorrências de palavras é afetada. Outra técnica que tem sido utilizada para driblar filtros Bayesianos é a utilização de "ASCII arte" e imagens para representar a mensagem.

Resumindo

Funcionar, funciona, pero...

» custo elevado em CPU
» retreinamento constante: o spammer se adapta!
» gera falsos positivos

Filtros de conteúdo

Bloqueio de anexos

Como muitos cavalos de tróia e vírus que afetam sistemas Windows são enviados, por exemplo, em arquivos executáveis (.exe) ou associados a certos aplicativos, como screen savers (.scr), alguns administradores procuram bloquear mensagens com determinados arquivos anexados.

O bloqueio pode ser feito com base no tipo ou no nome do arquivo, informações que podem ser obtidas no cabeçalho MIME. Os tipos dos anexos são dados pelo campo Content–Type: e os nomes dos arquivos pelo atributo 'name' deste campo.

Na prática, no entanto, esta técnica pode bloquear anexos que não são maliciosos, mas que estão entre os tipos proibidos, e pode deixar passar anexos que aparentemente não são hostis, como é o caso de imagens que exploram falhas no software usado para exibi–las.

Filtros de conteúdo

Considerações finais sobre filtros de conteúdo

Filtros de conteúdo podem consumir muitos recursos e produzir falsos positivos, que podem não ser identificados facilmente. Porém, anti–vírus em especial, podem ser bastante eficazes na detecção de códigos maliciosos.

Greylisting

Introdução

O conceito de greylisting consiste em recusar temporariamente uma mensagem e esperar por sua retransmissão, e parte dos seguintes princípios:

* que e–mails válidos são enviados a partir de MTAs legítimos, que mantém filas e possuem políticas de retransmissão em caso de erros temporários;
* spammers e códigos maliciosos raramente usam MTAs legítimos.

Contudo, existem spammers que utilizam MTAs legítimos ou mesmo reenviam as mensagens a fim de contornar esta técnica. Ainda assim, o greylisting tem se mostrado eficiente para barrar mensagens enviadas por vírus, worms e spam zombies.

O documento de referência sobre greylisting é o whitepaper *http://projects.puremagic.com/greylisting/whitepaper.html.*

Greylisting

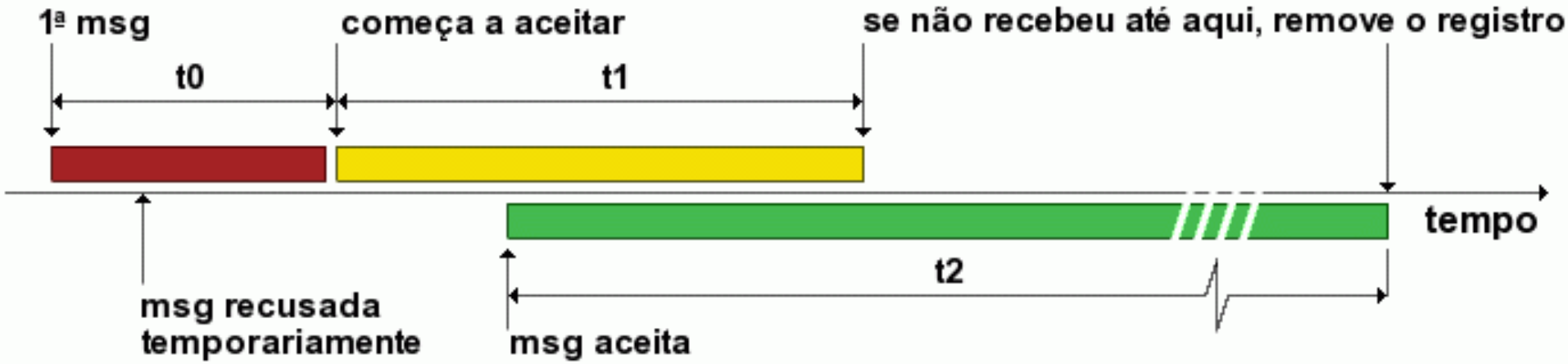
Funcionamento

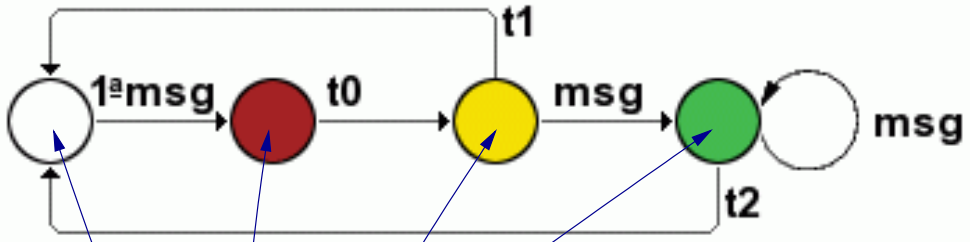
Em geral as implementações de greylisting mantém um banco de dados com registros indexados por:

*** endereço IP da origem;**
*** endereço do remetente no envelope;**
*** endereço do destinatário no envelope.**

Greylisting

Funcionamento (cont.)





transparente
aceitação temporária
bloqueio temporário
(IP,envelope) ainda não registrados no BD

Greylisting

Comentários finais

É importante também manter em uma lista branca, endereços IP que tem passagem livre pelo greylisting, ou porque são máquinas confiáveis (da própria rede, de redes conhecidas, etc) ou por que seus MTAs não conseguem tratar corretamente erros temporários.

Há um aspecto psicológico a ser considerado: as pessoas se acostumaram com a idéia (completamente equivocada) de que e-mail é instantâneo e podem se ver perdidas diante dos atrasos causados por esta técnica.

Há serviços de e-mail que tem vários endereços IP, o greylisting tratará a mesma mensagem vinda desses vários IPs como mensagens diferentes.

Se for possível reconhecer uma mensagem como boa por outro critério, não a submeta desnecessariamente ao "chá de cadeira".

SPF – Sender Policy Framework

Sumário

* Introdução
* Publicando a política SPF
* Configurando o MTA
* SPF e esquemas de retransmissão de e–mails
    * SRS – Sender Rewriting Scheme
    * Relays confiáveis
    * Redirecionamento
* Listas negras e SPF

SPF – Sender Policy Framework

Introdução

SPF é uma tecnologia para combater a falsificação de endereços de retorno dos e–mails (return–path). O mecanismo permite:

* ao administrador de um domínio: definir e publicar uma política SPF, onde são designados os endereços das máquinas autorizadas a enviar mensagens em nome deste domínio; e

* ao administrador de um serviço de e–mail: estabelecer critérios de aceitação de mensagens em função da checagem das políticas SPF publicadas para cada domínio.

O processo de publicação de uma política SPF é independente da implantação de checagem de SPF por parte do MTA, estes podem ou não ser feitos em conjunto.

SPF – Sender Policy Framework

Publicando a política SPF

Ao publicar uma política de SPF, o administrador de um domínio está autorizando determinados MTAs a enviar e–mails em nome deste domínio. O objetivo é evitar que terceiros enviem mensagem indevidamente em nome de seu domínio, e que mensagens de erro (bounces) causadas por spam com envelope falso sejam enviadas para o seu servidor.

Estas políticas são publicadas através de registros TXT do DNS, em formato ASCII. Um exemplo desse registro é:

Exemplo:

```
example.com.   IN      TXT      "v=spf1 a mx ip4:192.0.2.32/27 -all"
```

SPF – Sender Policy Framework

Publicando a política SPF (cont.)

```
example.com.    IN      TXT     "v=spf1 a mx ip4:192.0.2.32/27 -all"
```

Neste caso a política estabelece que pode enviar mensagens em nome do domínio example.com uma máquina que satisfaça um dos seguintes critérios:

* seu endereço IP deve ser um RR tipo A do domínio example.com (a);
* seja designada como MX do domínio example.com (mx); ou
* pertença ao bloco de endereços IP 192.0.2.32/27 (ip4).

A cláusula "-all" diz que devem ser recusados ("-", prefixo Fail) e-mails partindo de qualquer outro endereço IP (all).

SPF – Sender Policy Framework

Publicando a política SPF (cont.)

Todas as opções de prefixos são:

* "+" Pass
* "–" Fail
* "~" SoftFail
* "?" Neutral

O prefixo é opcional, e se omitido o valor utilizado é o "+" (Pass).

A cláusula "all" deve ser sempre a cláusula mais à direita. Ela define qual resposta será retornada em uma consulta SPF, caso nenhuma das outras cláusulas se aplique.

SPF – Sender Policy Framework

Publicando a política SPF (cont.)

O administrador de um MTA que consulte a política SPF do domínio do remetente de um e–mail, como definido no envelope, poderá rejeitar ou marcar como suspeita uma mensagem que não satisfaça à política SPF daquele domínio.

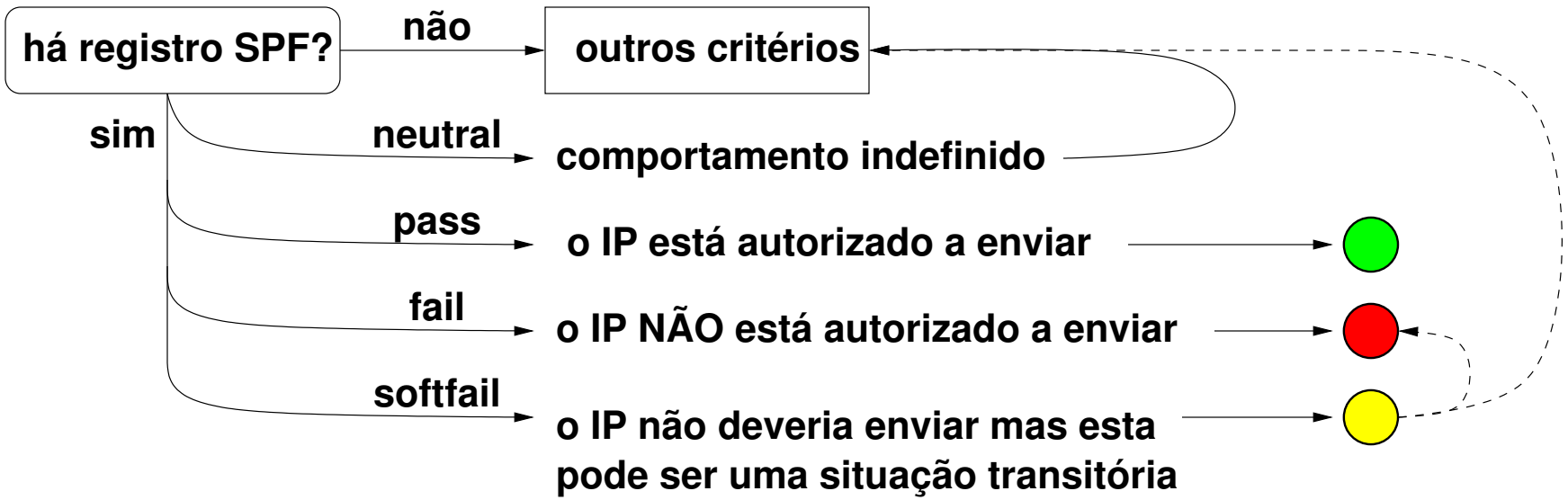
A especificação completa de como expressar uma política SPF pode ser encontrada no sítio de referência do SPF (http://www.openspf.org/) e no documento "Sender Policy Framework (SPF) for Authorizing Use of Domains in E–MAIL" (http://www.ietf.org/rfc/rfc4408.txt).

SPF – Sender Policy Framework

Configurando o MTA

A maioria dos MTAs atuais possui suporte a SPF, seja através de filtros externos (Milters), patches ou suporte nativo, via de regra usando a biblioteca libspf2.

É necessário estabelecer quais serão as ações tomadas dependendo da resposta obtida à consulta SPF. A RFC4408 define algumas possíveis interpretações dos resultados:



SPF – Sender Policy Framework

SPF e esquemas de retransmissão de e–mail

Mensagens legítimas, mas que tenham passado por um relay ou tenham sido redirecionadas, podem ser recusadas por MTAs que checam SPF. Para evitar que estas mensagens sejam rejeitadas, devem ser adotadas algumas estratégias, como SRS (Sender Rewriting Scheme) e autorizações especiais.

SPF – Sender Policy Framework

SRS – Sender Rewriting Scheme

Para evitar que MTAs que checam SPF rejeitem mails redirecionados, é necessário que o relay reescreva o endereço do remetente no envelope e encapsule o endereço original.

O SRS reescreve o endereço do remetente no envelope, de modo que:

* **o IP do transmissor é autorizado (pass) a enviar mensagens em nome do domínio à direita do "@";**
* **o endereço à esquerda do "@" permite determinar qual é o remetente real;**
* **o endereço à esquerda do "@" contém uma assinatura e um timestamp, que permitem reconhecer sua validade em mensagens de erro retornadas.**

SPF – Sender Policy Framework

SRS – Sender Rewriting Scheme (cont.)

Por exemplo, considere o remetente "fulano@example.com", cuja mensagem é retransmitida por "example.org", o envelope poderá ser reescrito da seguinte forma:

Exemplo:

```
SRS0=HHH=TT=example.com=fulano@example.org
```

onde,

* "HHH" é um hash criptográfico para validar os dados do envelope$
* "TT" é um timestamp.

SPF – Sender Policy Framework

SRS – Sender Rewriting Scheme (cont.)

Além de evitar o abuso por parte de spammers, estas informações, também permitem que o relay receba uma mensagem de erro, consiga validá–la e enviá–la para o endereço correto de origem.

Nem todos os MTAs têm suporte a esquemas de reescrita do endereço de remetente. Os que têm, quase sempre se baseiam na libsrs2 (http://www.libsrs2.org/).

De modo geral, somente servidores especializados em relays de mensagens é que precisam do SRS para poder operar em conjunto com SPF. Para outros tipos de MTAs, que estejam sob seu controle, há uma solução mais simples, apresentada a seguir.

SPF – Sender Policy Framework

Relays confiáveis

No caso de se usar MTAs secundários do tipo queue–only, o envio das mensagens do servidor secundário para o principal pode ser feito com SRS, mas há um esquema mais simples, que consiste em:

1. configurar o servidor secundário para também checar SPF, e tomar as mesmas ações que o servidor principal;

2. incluir o endereço IP do servidor secundário em uma lista branca de endereços IP previamente aprovados. Os MTAs que checam SPF normalmente possuem uma regra local para isso;

   ou

3. configurar o servidor secundário para que se autentique no servidor principal antes de iniciar as transações de envio das mensagens em sua fila.

SPF – Sender Policy Framework

Redirecionamento

O redirecionamento de mensagens através de esquemas como o uso do .forward ou de aliases redirecionando mensagens de um domínio para outro, também acarretam dificuldades quando o domínio tem um registro SPF.

Nesses casos é necessário reenviar o e–mail, reescrevendo o remetente no envelope, para evitar rejeição por parte de MTAs que chequem SPF.

SPF – Sender Policy Framework

Listas negras e SPF

Caso seja feito o uso de listas negras, é interessante verificar se o endereço IP do remetente se encontra em uma lista negra somente depois de verificar o registro SPF. Caso o resultado do SPF for Pass, o IP não deve ser bloqueado.

Esta recomendação é importante porque listas negras possuem uma taxa relativamente alta de falsos positivos, como discutido na seção sobre listas de bloqueio.

Nem todos os MTAs, entretanto, permitem que se faça a consulta à lista negra depois de verificar o SPF. É possível usar as políticas padrão do SPF para implementar consultas a listas negras, embora sejam configurações não triviais. No sítio de referência do SPF (http://www.openspf.org/) há vários exemplos.

DKIM – Domain Keys Identified Mail

DKIM é uma iniciativa conjunta da Yahoo! e da Cisco que, embora ainda seja pouco usada, tem potencial para ser um mecanismo eficiente de combate ao spam. Consiste em assinar as mensagens com uma chave pública, certificada ou não, para garantir a autenticidade do remetente. Ao contrário do SPF, que verifica o envelope, o DKIM verifica o cabeçalho da mensagem. Esta técnica acarreta um custo computacional adicional por mensagem, tanto para o MTA remetente quanto para o MTA destino.

Para habilitar DKIM é necessário:

* **criar um par de chaves pública e privada (o OpenSSL pode ser usado para isso);**
* **deixar a chave pública disponível via DNS, de forma semelhante à publicação da política do SPF;**
* **colocar a chave privada no MTA responsável pelo envio das mensagens;**

DKIM – Domain Keys Identified Mail

Assinando e verificando mensagens

Para utilizar DKIM no envio de mensagens basta assinar cada mensagem enviada com a chave privada colocada no MTA. Esta assinatura é enviada como um campo adicional do cabeçalho.

Para verificar a autenticidade de uma mensagem recebida é necessário:

*** obter a chave pública do domínio do From:, via DNS,**
*** verificar a assinatura da mensagem;**

DKIM – Domain Keys Identified Mail

Assinando e verificando mensagens (cont.)

O resultado da verificação da assinatura pode chegar a uma das três conclusões:

* a assinatura é válida, a mensagem vem realmente do domínio indicado no campo From: e pode então ser avaliada por outras técnicas anti–spam;
* a assinatura não é válida, a mensagem pode ser marcada como suspeita ou ser recusada;
* o domínio do remetente não possui um registro DKIM, não sendo possível usar a informação de DKIM como critério de decisão.

DKIM – Domain Keys Identified Mail

Informações adicionais

Mais detalhes sobre DKIM, bem como softwares de suporte, podem ser obtidos em:

* **DomainKeys: Proving and Protecting Email Sender Identity http://antispam.yahoo.com/domainkeys.**

A motivação do protocolo e o tipo de problema que ele foca são discutidos em http://www.ietf.org/rfc/rfc4686.txt

Quadro comparativo

técnica	alvo	falso positivo?	falso negativo?	popularidade
listas de bloqueio	endereços IP de spammers	SIM, MUITO	NÃO	alta
filtros de conteúdo	padrões em mensagens	SIM	SIM	alta
greylisting	entrega direta (spambots)	UM POUCO	NÃO	média
SPF	amarrar IP + domínio do envelope	NÃO	NÃO	média
DKIM	autenticar o remetente no cabeçalho	NÃO	NÃO	experimental

Boas práticas de configuração para evitar abusos

Vários serviços Internet, não somente o correio eletrônico, estão relacionados com o envio e recebimento de spam, bem como com sua prevenção. O administrador de redes tem que estar atento para as interações, por vezes intrincadas, entre os vários serviços e o correio eletrônico.

Os seguintes subsistemas tem implicação na questão do spam:

- Correio Eletrônico (óbvio)
- Servidores Web (já vimos por que)
- Servidores de Nomes
- Serviços de Proxy
- Firewalls

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Sumário

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Introdução

Configuração: um servidor concentrador que atende a um grupo de estações clientes.

Objetivos:

*** fazer com que as mensagens enviadas passem pelo servidor; e**
*** evitar que mensagens saiam clandestinamente, sem passar por ele.**

O administrador do serviço também tem que tratar de corrigir falhas, normalmente percebidas por terceiros. Para isso temos que estar com os "ouvidos" abertos, o que significa ter endereços de correio prontos para receber reclamações e reagir a essas reclamações.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Relays abertos

Relays abertos são MTAs que transmitem mensagens de qualquer domínio, ou mesmo só de domínios determinados, para qualquer outro, sem pedir autenticação, sem restringir (ou restringindo muito pouco) a faixa de endereços IP de origem.

Os relays abertos são utilizados por spammers pelo fato de proverem anonimato. Para o responsável pelo MTA com relay aberto sendo abusado, as conseqüências são o consumo de recursos e a possível inclusão do MTA em listas de bloqueio. Além disso, ele pode passar a receber mensagens de erro e reclamações sobre os spams enviados via seu MTA.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Relays abertos (cont.)

É importante, ao configurar um MTA, restringir ao máximo os endereços IP que tem permissão para usá–lo como relay, se possível limitando ao localhost. Na seção sobre servidores Web são discutidas implicações na liberação do localhost para uso do relay.

Antes de tornar um serviço de correio eletrônico público é fundamental verificar se ele está se comportando como relay aberto. Uma maneira fácil de fazer isso é através de um telnet pela porta adequada, digitando os comandos SMTP diretamente. A ferramenta openssl, com o comando s_client, pode ser usada no caso de sessões cifradas.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Relays abertos (cont.)

```
myhost:~$ telnet mailserver.example.com 25
Trying 192.0.2.82...
Connected to mailserver.example.com.
Escape character is '^]'.
220 babbo.example.com ESMTP Sendmail 8.13.4/8.13.4; Tue, 20
 Sep 2005 16:31:04 -0300
helo myhost.example.net
250 babbo.example.org Hello IDENT:1008@myhost.example.net
 [192.0.2.44], pleased to meet you
mail from: <john.doe@example.net>
250 2.1.0 <john.doe@example.net>... Sender ok
rcpt to: <fulano@example.edu>
550 5.7.1 <fulano@example.edu>... Relaying denied. Proper
 authentication required.
quit
221 2.0.0 babbo.example.com closing connection
```

Boas práticas de configuração para evitar abusos

Correio Eletrônico

SMTP autenticado

Normalmente o protocolo SMTP trabalha sem utilizar autenticação e não diferencia se a conexão está sendo feita por um cliente ou por outro MTA. A falta de autenticação por parte de um cliente ao utilizar o MTA para o envio de mensagens pode facilitar o envio de spam ou o abuso por parte de spammers.

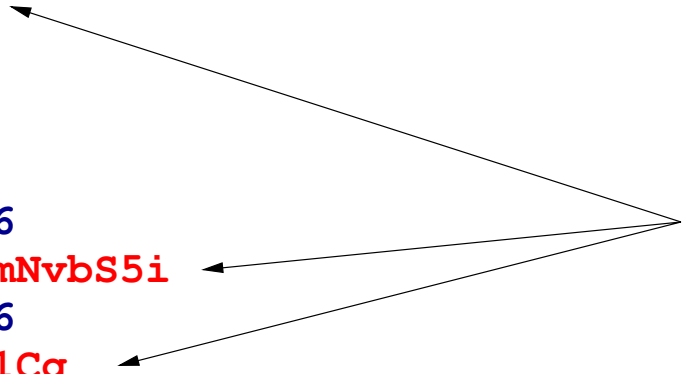
Para evitar esse tipo de abuso uma das medidas é exigir que qualquer cliente, independentemente do endereço IP de origem, apresente credenciais de acordo com a RFC 2554, a não ser que o destino da mensagem seja local.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

SMTP autenticado (cont.)

```
$ telnet post-office 25
Trying 200.231.48.36...
Connected to post-office.
Escape character is '^]'.
220 InterNexo MTA. ESMTP
ehlo pumba
250-InterNexo MTA.
250-AUTH=LOGIN
250-AUTH LOGIN
250-PIPELINING
250 8BITMIME
auth login
334 VXNlcm5hbWU6
51bmVzI2luZXhvLmNvbS5i
334 UGFzc3dvcmQ6
cHV0YXF1ZXBhcml1Cg
235 go ahead
mail from: <danton.nunes@inexo.com.br>
250 ok
.....
```



credenciais em Base64
MUITO inseguro!!

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Porta de submissão (587/TCP)

Uma configuração que é bastante efetiva contra abusos consiste em reservar a porta 25/TCP somente para troca de mensagens entre MTAs e usar a porta 587/TCP para mensagens enviadas por um cliente para o seu MTA. Costuma–se usar o termo MSA (Mail Submission Agent) para o MTA configurado para responder pela porta 587/TCP.

Para a utilização da porta de submissão, onde a autenticação é obrigatória, é necessário que todos os MUAs dos clientes reconfigurados para a utilização da nova porta e fornecimento de credenciais.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Servidores secundários

Para evitar que servidores secundários sejam abusados por spammers, alguns cuidados devem ser tomados ao configurá–los:

* todas as medidas anti–spam adotadas no servidor principal, como SPF, greylisting, etc, devem, na medida do possível, ser implementadas no servidor secundário também.

* o servidor secundário deve saber para quais domínios ele pode fazer relay. Este servidor não deve ser configurado como 'null relay client'.

* o servidor principal deve assumir que o servidor secundário é confiável, e não fazer testes de SPF nem colocar em greylisting mensagens que venham dele.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Endereços especiais

A RFC 2142 (Mailbox Names for Common Services, Roles and Functions) prevê um conjunto de endereços especiais, que devem ser configurados como aliases para os e–mails do pessoal responsável pelas áreas específicas.

* abuse: para tratar de comportamento inapropriado ou abusivo, como envio de spam;
* noc (Network Operations Center): para questões sobre infra–estrutura operacional;
* security: para questões relacionadas a segurança;
* postmaster: funcionalidade definida nas RFCs 2821 e 2822.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Endereços especiais (cont.)

Não basta ter esses endereços definidos, eles precisam ser lidos regularmente pelo pessoal responsável pelas áreas afins. As mensagens enviadas, especialmente para abuse e security devem ser tratadas com atenção, pois provavelmente indicam problemas em sua rede que devem ser remediados o quanto antes.

Convém que esses endereços permaneçam em uma lista branca, livres de filtros e proibições, caso contrário mensagens importantes, contendo notificações de spam, phishing ou ataques partindo de sua rede poderão não ser recebidas. Além disso, outras mensagens notificando problemas de configuração da rede ou no funcionamento do correio eletrônico e nas próprias regras anti–spam, poderão ser bloqueadas.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Servidores Web

Servidores Web podem ser abusados para enviar spam dependendo dos serviços disponíveis, portanto o administrador de sites também é responsável pela prevenção. As fontes de abuso mais comuns são o envio de mensagens através de formulários e funções de linguagens de geração de conteúdo dinâmico capazes de enviar e–mail.

Spam vindo de servidores Web são particularmente difíceis de combater, porque eles vem de MTAs legítimos, com fila e retransmissão, e com envelopes consistentes com o endereço IP, passando assim tanto por greylisting quanto por teste de SPF. Por conta disso a ação preventiva nestes casos é fundamental.

Boas práticas de configuração para evitar abusos

Correio Eletrônico

Servidores Web (cont.)

O maior problema está na possibilidade de scripts e servlets enviarem mensagens. Essa possibilidade é tão desejável quanto perigosa.

Não há mecanismo 100% efetivo para impedir que um servidor Web envie mensages para qualquer lugar, afinal, ele roda como um usuário. Algumas ações:

- Programação defensiva: não confiar em qualquer dado de fora.
  depende da boa vontade dos programadores de scripts.
  deveria ser prática comum de programação, mas não é.
- Uso de agentes de submissão especiais.
  "wrappers" para o MSA regular, p.ex. simulador de qmail–inject, que só passam adiante mensagens em que destinatários se encontrem em uma lista administrada.

Boas práticas de configuração para evitar abusos

Servidores de nomes

Os dois problemas com DNS mais relacionados com spam e e–mail em geral são:

- **Zonas Reversas**
- **Registros de SPF e DKIM**

Boas práticas de configuração para evitar abusos

Servidores de nomes

Zonas reversas

Uma das técnicas de bloqueio existentes leva em consideração o fato de um IP não possuir endereço reverso. Muitas vezes também é levado em conta se o nome da máquina, retornado pela consulta ao endereço reverso do IP, possui um registro do tipo A que seja igual ao endereço IP originalmente consultado. Em função disso, é importante que a configuração das zonas direta e reversa de um domínio sejam feitas corretamente.

A zona reversa é delegada a redes que sejam sistemas autônomos (AS) e possuam seus próprios blocos de endereços IP. Sendo que este AS pode sub–delegar a zona reversa aos seus clientes.

Boas práticas de configuração para evitar abusos

Servidores de nomes

Zonas reversas (cont.)

três casos possíveis

1. o provedor não delega a zona reversa: neste caso é necessário solicitar ao provedor que configure a zona reversa de maneira consistente com a direta;

2. o provedor delega a zona reversa e o bloco de endereços é /24 ou maior: neste caso é possível configurar a zona in.addr–arpa corretamente em seu próprio servidor de nomes, bem como a zona direta correspondente.

3. o provedor delega a zona reversa e o bloco de endereços é menor que /24: neste caso deve ser usado o procedimento descrito na BCP 20 (ou RFC 2317, Classless IN–ADDR.ARPA delegation), de acordo com convenções adotadas pelo seu provedor e com as instruções por ele fornecidas.

Boas práticas de configuração para evitar abusos

Servidores de nomes

Registros de SPF e DKIM

Outros aspectos de configuração de DNS, que afetam sistemas robustos de correio eletrônico, são os registros de SPF e de DKIM que devem ser feitos através de registros do tipo TXT.

Exemplos:

Registro de SPF:

```
example.net.   IN   TXT   "v=spf1 a mx ip4:192.0.2.32/27 -all"
```

Registro de DKIM:

```
mail._domainkey.example.net.  IN  TXT  "g= k=rsa t=y p=MF...XYZ"
```

Boas práticas de configuração para evitar abusos

Servidores proxy

Outro serviço que, se mal configurado, pode ser abusado para envio de spam é o serviço de proxy.

Além dos comandos usuais de HTTP, os proxies como o Squid, implementam um comando CONNECT que permite ao usuário estabelecer conexões genéricas através do proxy, entre elas, sessões de SMTP. O comando CONNECT é necessário porque há recursos na Web que não são acessíveis pelo protocolo HTTP.

O administrador de um serviço de proxy deve tomar cuidado para evitar que o comando CONNECT fique publicamente disponível. De uma maneira geral, o acesso a esse comando deve ser restrito às portas 443 (HTTPS) e 563 (NEWS), e somente para a rede interna da corporação.

Proxies transparentes não precisam do CONNECT: desabilite–o!

Boas práticas de configuração para evitar abusos

Firewalls

Clientes internos

Spam zombies, worms e vírus costumam se conectar diretamente aos MTAs dos domínios vítimas, portanto, bloquear a saída para a porta 25/TCP em um firewall pode ser bastante efetivo para impedir o envio de e–mails a partir das máquinas infectadas. A análise dos logs do firewall pode indicar quais máquinas da rede interna estão possivelmente sendo abusadas e envolvidas no envio não autorizado de e–mails.

É importante que esta regra de bloqueio não se aplique aos MTAs legítimos da sua rede. No caso de provedores, o bloquio não deve ser aplicado aos MTAs de clientes corporativos.

Vale lembrar que os firewalls podem fazer muito pouco para prevenir a contaminação de máquinas de usuário. por que?

Boas práticas de configuração para evitar abusos

Firewalls

Usuários em viagem

Um caso importante a se considerar são usuários viajantes, que não estão na rede interna. Caso a máquina de um destes usuários seja contaminada, pode haver tentativas de transmissão de mensagens. Ações preventivas:

1. instalar firewall pessoal que bloqueie a saída pela porta 25/TCP, conectar no MSA autorizado pela porta 587.

2. adicionalmente estabelecer uma rede virtual privativa (VPN) com a sede.

3. Como esta máquina estará freqüentemente em redes inseguras, convém utilizar as versões cifradas (sob TLS) dos protocolos SMTP, POP ou IMAP. As portas das versões não cifradas destes protocolos devem ser bloqueadas no firewall pessoal.