TRACE e o Correio Multimídia

**Ricardo Campanha Carrano, Antonio Caminada,
Débora Christina Muchaluat-Saade, Luiz Claudio Schara Magalhães**

Departamento de Engenharia de Telecomunicações - Universidade Federal Fluminense
Rua Passo da Pátria 156, Niterói, RJ

{carrano, antonio, debora, schara}@midiacom.uff.br

Abstract. *Despite its ubiquity, the Internet Electronic Mail System still harbors some pending issues that limit its wide acceptance as an effective multimedia transport platform. In this article we identify some of these issues and demonstrate that the propositions based on the recipient-pull model, in lieu of the current sender-push model, represent the best approaches to address these problems and we highlight the TRACE model.*

Resumo. *Apesar da ubiqüidade alcançada, o correio eletrônico da Internet ainda convive com uma série de problemas que limitam seu emprego como plataforma efetiva para o envio de conteúdo multimídia. Neste texto, identificaremos alguns desses entraves e demonstraremos que as proposições baseadas na reversão do modelo de transporte de sender-push para recipient-pull - com destaque para o TRACE - são um componente fundamental na solução desses problemas.*

1. Introdução

Nas últimas duas décadas, o modelo de transporte de correio eletrônico da Internet, apesar da notável ubiqüidade alcançada e, também, apesar das radicais mudanças em seu perfil de uso, conseguiu permanecer fundamentalmente inalterado. O protocolo SMTP [Postel 1982] foi ampliado, incorporando novos comandos e funcionalidades [Klensin 2001], mas manteve-se, em seu aspecto mais marcante, o mesmo. Ele ainda se baseia em um sistema de remessa de mensagens do tipo *store-and-forward.*

São vários e distintos os problemas que impedem a adoção do correio eletrônico da Internet como efetiva plataforma para o transporte de multimídia. Em primeiro lugar, temos problemas de caráter geral que afetam todos os conteúdos transportados. Nesta linha destacamos os problemas de privacidade e de autenticidade. Sendo o segundo crítico, sobretudo por sua implicação direta com um outro problema bastante atual do correio eletrônico: o *spam.*

Na categoria dos problemas específicos do conteúdo multimídia, observamos que as mensagens de correio eletrônico, formadas de corpo e cabeçalho [Resnick 2001], mesmo após a introdução do MIME [Freed 1996], carecem de estruturas semânticas mais elaboradas e, por último, destacamos a falta de otimização do modelo vigente. Isto é, quando uma mesma mensagem é enviada para um conjunto de *n* destinatários, são transmitidas e armazenadas *n* cópias desta mensagem.

As diversas soluções para os problemas acima mencionados atacam apenas pontualmente os problemas do correio eletrônico. O emprego de criptografia [OpenPGP 2006], [S/MIME 2006], [Hoffman 2002], por exemplo, é visto como uma solução natural para as questões de segurança, ao passo que filtros [Sahami 1998], cobrança de tarifas [E-Postage 2006], técnicas de autenticação baseadas em DNS [DBSL 2006], [RFC-Ignorant.Org 2006], [SPF 2006], a extensão do SMTP [Hoffman 2002], [Duan 2005], ou mesmo sua completa substituição [IM2000 2006], [AMTP 2006], além de outras técnicas de coerção procuram combater o *spam*. Mas nenhuma dessas técnicas dá conta de todos os problemas acima identificados.

Nesse artigo demonstramos como a adoção do chamado modelo *pull* e, mais especificamente do TRACE, pode eliminar ou minimizar estes problemas. Na seção 2, apresentaremos a proposta do projeto TRACE, em seguida iremos situar o TRACE no cenário de outras propostas (seção 3). Nossas conclusões são apresentadas na seção 4.

2. O Projeto Trace

O projeto TRACE [Caminada 2005] é uma proposição do Laboratório Mídiacom da Universidade Federal Fluminense e, como outras soluções [Duan 2005], [Turner 2000], [SMHMS 2006] aos problemas do correio eletrônico, emprega o modelo *pull* para o transporte do correio eletrônico. Diferente de outras soluções, o TRACE não propõe, para tal, qualquer alteração ou extensão do protocolo SMTP.

Na realidade, como veremos adiante, o modelo de transporte em uso atualmente (Figura 1) é mantido compatível e mesmo os MTAs em uso corrente podem ser utilizados no modelo com a simples adição de um componente TRACE intermediário (TRACE-Proxy), responsável por separar a mensagem em suas partes (cabeçalho e corpo) e, então, utilizar o MTA instalado para envio da mensagem TRACE. Esta, inclusive, é a forma utilizada para testes do sistema no Laboratório Midiacom.

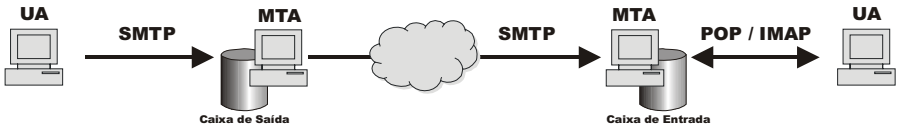

Figura 1: Sistema de Transporte de Correio Eletrônico na Internet

O corpo da mensagem TRACE consiste basicamente de um endereço universal (URL) da mensagem original, a ser recuperada através do protocolo HTTP e tratável, portanto, por praticamente qualquer agente de usuário, o que representa a vantagem da compatibilização automática da base de usuários.

O TRACE implementa suas funcionalidades através de dois processos (ver Figura 2): um para dividir a mensagem (separar o cabeçalho do corpo) e enviar o cabeçalho para o destinatário, o TRACE-proxy; e um outro para gerenciar a entrega do corpo, o TRACE-server. Esse último transfere a mensagem quando essa é requisitada, apaga mensagens expiradas e efetua a autenticação de segurança. O *back-end* consiste, assim, desses dois componentes servidores.

O primeiro componente (TRACE-proxy) analisa a mensagem original, separando o cabeçalho do corpo. Ao cabeçalho, ele adiciona o ID dessa mensagem, que é usado pelo destinatário para recuperar o corpo da mensagem. O mesmo ID é

adicionado ao corpo. Este ID é composto de duas partes: uma que é o identificador de armazenamento, para possibilitar a recuperação da mensagem, e outra, usada para criptografar o corpo da mensagem, conforme será explicado a seguir, para aumentar a privacidade das mensagens armazenadas. Este novo cabeçalho contém, ainda, uma lista dos arquivos anexados (se houver) e um link HTTP para o corpo da mensagem.

O segundo componente (TRACE-server) é responsável pela entrega do corpo da mensagem, quando esse é solicitado pelo destinatário. Esse processo é executado no repositório distribuído, que pode ser uma máquina distinta do MTA do remetente ou não. Ele faz a autenticação do destinatário por intermédio do ID da mensagem, de modo que esse seja o único a ter permissão para ver o seu conteúdo. Para evitar o acúmulo de mensagens, muitas vezes esquecidas pelos destinatários, esse processo também executa um "coletor de lixo", que apaga mensagens após um certo tempo. Ao serem enviadas, as mensagens ganham um "prazo de validade".

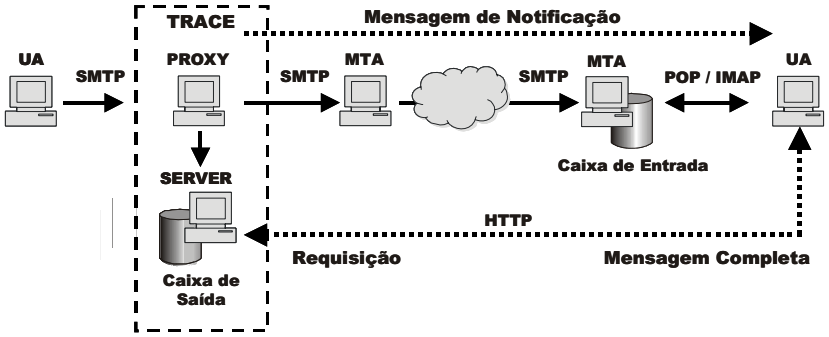

Figura 2: Sistema de Transporte proposto pelo TRACE

Os arquivos anexados são listados no cabeçalho que vai para o destinatário. O corpo da mensagem contém um link para o(s) arquivo(s), para que esses possam ser vistos. Quando é feita a requisição HTTP, eles são enviados e exibidos no browser ou no programa apropriado (ou, então, o usuário pode optar por fazer o download do arquivo), conforme já acontece hoje quando é feita a solicitação de um arquivo a um servidor HTTP.

Para garantir que somente o usuário a quem a mensagem se destina possa lê-la, é usado um esquema de autenticação. Ao ser feita a divisão da mensagem, um identificador é criado e gravado tanto na mensagem quanto no cabeçalho, e este é usado como chave para a criptografia da mensagem. Ao clicar no link para ver a mensagem, esse identificador é retornado e somente com ele a mensagem pode ser descriptografada. Para aumentar a segurança da mensagem, é possível adicionar um esquema de chave privada/chave pública, pois assim nem a captura da mensagem de notificação permitiria a leitura da mensagem, e a mensagem pode ir criptografada até o destino. Se o remetente conhecer a chave pública do destinatário, a mensagem é primeiro criptografada usando essa chave e, depois, a parte do identificador da mensagem é usada para a criptografia. O identificador é um número de 512 bits escolhido aleatoriamente, de forma a dificultar ataques à base de dados (na qual um atacante tentaria ler mensagens pedindo mensagens em seqüência).

Após ser feita a divisão da mensagem, o cabeçalho (com os campos adicionais) segue o caminho convencional de um correio eletrônico hoje, isto é, segue via SMTP

pela rede até o MTA (servidor SMTP) do destinatário e deste para o servidor POP ou IMAP, de onde será transferido pelo usuário para sua máquina. Como o cabeçalho normalmente será bem menor que a mensagem completa, isso permite seu envio a terminais com memória limitada, como telefones celulares e PDAs.

Além dos servidores já desenvolvidos, o projeto TRACE prevê o desenvolvimento de um cliente especializado. Apesar da mensagem TRACE ser compatível com os MUAs atuais, algumas vantagens podem ser alcançadas com um agente de usuário específico. Um exemplo seria uma maior facilidade de incorporar criptografia ao modelo, seja para garantia de sigilo da mensagem ou para verificação de autenticidade do remetente. Outra possibilidade seria a incorporação de capacidades de edição e visualização de documentos SMIL.

O TRACE tem, dessa forma, um efeito colateral desejável: a possibilidade de incorporação prática de soluções de segurança e de técnicas de composição de mensagens, utilizando, para tal, apenas padrões abertos.

Finalmente, a proposta do TRACE é ortogonal a outras propostas de diminuição de *spam* [Freed 1996], [DSBL 2006], e pode ser implementada concorrentemente, trazendo no mínimo a diminuição do tráfego na rede, já que mensagens identificadas como *spam* não serão requisitadas e não ocuparão espaço nos servidores de correio dos destinatários. O TRACE também equipara o serviço de email aos outros serviços consagrados na Internet que, utilizando o modelo *pull*, representam um modelo de transporte mais justo, no qual o maior ônus recai sobre o autor.

3. O Trace e outras propostas

Uma vantagem da proposta TRACE é sua imediata compatibilidade. O TRACE não introduz qualquer mudança nos protocolos de comunicação envolvidos (SMTP e HTTP) como fazem o IM2000 [IM2000 2006] ou, em menor escala, o DMTP [Duan 2005] e outras soluções baseadas na extensão do SMTP. Como dissemos, substituir ou mesmo alterar um protocolo de ampla aceitação na Internet apresenta grandes dificuldades.

Por outro lado, o TRACE não ataca explicitamente o problema da semântica das mensagens hipermídia como faz o SMHMS [SMHMS 2006]. Mas o último é bastante mais complexo em sua arquitetura, de onde se justifica o surgimento do MMM [Batista 1996], em muitos aspectos similar ao TRACE e também ao CM email [Turner 2000].

Neste ponto é oportuno fazer a distinção entre o método usado para a mensagem de notificação e a linguagem utilizada na composição da mensagem. Parece natural que a mensagem de notificação utilize o conceito de URL e de *hyperlink* para apontar para a mensagem original, mas isso de forma alguma implica em restrições aos métodos de construção da mensagem referenciada.

Assim, tanto TRACE como MMM ou CM email poderiam definir qualquer linguagem de composição para esse efeito. Ou não definir nenhuma, já que o maior entrave a ser removido está ligado ao método de transporte das mensagens, e o problema do formato passa a ser independente do correio eletrônico propriamente dito, uma vez que a mensagem de notificação pode referenciar a qualquer tipo de objeto ou composição.

O princípio de trazer o máximo de melhorias com o mínimo de alterações na infra-estrutura pré-existente reforça a idéia de implementar as mudanças através da interposição de uma camada adicional entre MUA e MTA. Essa é a proposta do GNU Anúbis [Anúbis 2006] e também do TRACE.

Em suma, o TRACE ataca primariamente as questões de eficiência e justiça (ônus do armazenamento) e tem como seu principal trunfo a simplicidade e a ortogonalidade a diversas outras propostas de melhoria do modelo de correio eletrônico, particularmente as de combate ao *spam* [Freed 1996], [DSBL 2006], [RFC-Ignorant.Org 2006]. [E-Postage 2006], [SPF 2006].

4. Conclusão

As diversas propostas aqui apresentadas, para melhoria do correio eletrônico da Internet, baseiam-se na idéia de que o modelo *sender-push*, hoje vigente, é inadequado e propõem a adoção do paradigma utilizado pela maioria das aplicações cliente-servidor da Internet atual – o modelo *pull*.

Apesar de algumas propostas apresentarem maneiras de incorporar o modelo *pull* através da substituição ou extensão dos protocolos pré-existentes, um caminho mais trilhado tem sido a incorporação de elementos da World Wide Web ao cenário do transporte de correio eletrônico. A maioria destas soluções objetiva atacar primariamente o problema do *spam* e, como efeito colateral, a questão do desperdício de recursos resultante do envio e armazenamento de mensagens replicadas. Mas, é fato que a adoção isolada do paradigma *recipient-pull* não resolve o problema da composição das mensagens multimídia e também não é condição obrigatória para o emprego de criptografia.

Esperamos ter mostrado que o problema do formato e da composição das mensagens é ortogonal aos demais problemas apresentados. Assim, acreditamos que o emprego de uma linguagem de composição multimídia (como SMIL [SMIL 2006]) aliado à interposição de um Proxy (entre MUA e MTA) que venha a implementar o modelo *pull* e incorpore, ao mesmo tempo, técnicas de criptografia de chave pública, pode representar um enorme avanço para o correio eletrônico. E isso tudo preservando toda a infra-estrutura subjacente atual.

Simultaneamente com a distribuição das contas para alunos da Engenharia da UFF para testes de usabilidade, está sendo desenvolvido um cliente TRACE que permitirá a composição em SMIL e implementará funcionalidades como a criação de uma lista branca para a busca automática de mensagens de remetentes que sejam caracterizados como confiáveis.

Referências

Postel, J. (1982) “RFC 821 - Simple Mail Transfer Protocol”

Klensin, J. (2001) “RFC 2821 - Simple Mail Transfer Protocol”

Caminada, A; Magalhaes, L; (2005) PULL: “Um novo modelo para o Correio Eletrônico.” In: XXII Simpósio Brasileiro de Telecomunicações (SBrT'05), 2005

OpenPGP - IETF OpenPGP working group - http://www.ietf.org/html.charters/openpgp-charter.html (acessado em 20/12/2006)

S/MIME - S/MIME Mail Security - http://www.ietf.org/html.charters/smime-charter.html (acessado em 20/12/2006)

GNU Anubis - Free Software Foundation (FSF) - http://www.gnu.org/software/anubis/ (acessado em 20/12/2006)

Freed, N; Borenstein N. (1996) “RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies”

DSBL Distributed Sender Blackhole List - http://dsbl.org/main. (acessado em 20/12/2006)

RFC-Ignorant.Org - http://www.rfc-ignorant.org (acessado em 20/12/2006)

E-Postage - Method for Controlling Spam Via E-Postage Fees - http://www.mall-net.com/spam/ (acessado em 20/12/2006)

IM2000 - http://www.im2000.org/ (acessado em 20/12/2006)

SPF - Sender Frame Policy – www.spf.org (acessado em 20/12/2006)

Hoffman, P. (2002) “RFC 3207 - SMTP Service Extension for Secure SMTP over Transport Layer Security”

Duan, z.; Gopalan, k; Dong, Y. (2005) "DMTP: Controlling Spam Through Message Delivery Differentiation"

Resnick P. (2001) “RFC 2822 - Internet Message Format”

Turner, David A.; Ross, Keith W. (2000) "A Comprehensive Architecture for Continuous Media E-mail".

SMHMS: Um Correio Eletrônico Multimídia/Hipermídia - ftp://ftp.telemidia.puc-rio.br/pub/docs/conferencepapers/1994_05_SOARES.pdf (acessado em 20/12/2006)

Batista, T.; Rodriguez, N. de La Rocque; Soares, L. F. Gomes, Resende, M.C. (1996) "MMM: Um Correio Eletrônico Multimídia sobre o WWW"

SMIL - The Synchronized Multimedia Integration Language - http://www.w3.org/AudioVideo/ (acessado em 20/12/2006)

Sahami,M;, Dumais, S; Heckerman, D; Horvitz, E (1998). A Bayesian approach to filtering junk e-mail. AAAI'98 Workshop on Learning for Text Categorization.

AMTP – Authenticated Mail Transfer Protocol - http://amtp.bw.org/docs/ (acessado em 20/12/2006)