



INFORMÁTICA

Máscaras na Internet

Sistema desenvolvido na UFMG permite controlar a privacidade na rede mundial de computadores

LILIANE NOGUEIRA

Pouca gente se dá conta da maior facilidade em manter a privacidade no mundo real do que no, cada vez mais complexo, mundo on-line. Além dos hackers que invadem computadores de usuários e servidores, os próprios provedores (empresas que hospedam sites e contas de e-mails) e qualquer endereço na Internet também podem coletar dados, de forma sistemática, com a finalidade de personalizar serviços ou de bisbilhotar a vida alheia. Ao acessar a rede mundial de computadores, o usuário pode, por meio do preen-

chimento de formulários, fornecer dados pessoais como endereço, telefone, número da identidade ou do cartão de crédito, além de dar informações, sem saber, sobre seus interesses, costumes, compras e preferências pessoais. Preocupados com a perda de privacidade dos milhões de internautas que acessam a Internet e não querem ser identificados, pesquisadores do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG) desenvolveram um sistema que permite navegar pela rede com mais privacidade, protegidos por "máscaras".

Uma máscara é um tipo de pseudônimo associado a um grupo de pessoas que compartilham um mesmo tema de interesse, em vez de estar associada a um indivíduo específico. Assim, de forma automática, o usuário ao se conectar a um site sobre turismo, por exemplo, fica ligado a um grupo identificado ao tema, no próprio provedor. Os mantenedores do site registram a visita do grupo e não do usuário que poderá receber informações personalizadas, se for o caso, sem nenhum tipo de identificação.

O trabalho da equipe da UFMG ganhou notoriedade. Foi capa da revista

Security&Privacy (Segurança e Privacidade), uma das mais importantes publicações da área nos Estados Unidos, editada pelo *Institute of Electrical and Electronics Engineers* ou Instituto de Engenheiros Eletricistas e Eletrônicos, organização mais conhecida pela sigla IEEE, que reúne 380 mil membros em 150 países, nas áreas de engenharia, telecomunicações e computação. O artigo *Masks: bringing anonymity and personalization together* (*Máscaras: conjugando anonimato e personalização*) foi escrito pelos pesquisadores Virgílio Almeida e Wagner Meira Júnior, professores da UFMG, e pela doutoranda Lucila Ishitani. O protótipo estará disponível como software livre, de forma gratuita, para usuários e instituições – universidades, governo, empresas e provedores – ainda este ano.

Perfil valioso - O problema da falta de privacidade na Internet é grave porque muitos internautas desconhecem que a rede mundial aloja programas camuflados, capazes de monitorar o comportamento e traçar o perfil dos usuários. O simples fato de acessar um portal já é o suficiente para ser identificado. Segundo Almeida, os *pop-ups*, aquelas janelinhas com publicidade que se abrem na tela independente da escolha do usuário, além de irritantes, identificam de forma compulsória os computadores conectados à página, antes mesmo de serem fechados. Não é necessário nenhuma ação do internauta para que exista essa invasão. Quanto aos *banners* (os espaços de publicidade dentro de um site), basta clicar sobre eles e, automaticamente, as informações sobre a máquina podem ser capturadas.

Uma das formas de monitorar o comportamento e preferências dos usuários é através dos *cookies* – arquivos armazenados por sites no computador do usuário – com o objetivo de tornar possível identificar o internauta que acessa as páginas virtuais, bem como recuperar as atividades anteriores desse usuário, arquivadas no servidor do site. Esses arquivos são instalados no computador do usuário, independente da vontade do mesmo e sem que ele sequer perceba, no momento em que aces-

sa um site. “Na verdade, a identificação do internauta é realizada usando recursos do navegador, tanto do Netscape quanto do Explorer” diz Meira Júnior, explicando que os *cookies* estão atrelados a eles. Outra forma de ser identificado é através do endereço IP, Internet Protocol, que é o registro dos usuários nos respectivos provedores presente em todas as interações do usuário na rede.

Atualmente, o internauta pode facilmente recorrer a ferramentas para não ser identificado, como as que desativam os *cookies* nos próprios navegadores, mas fica totalmente anônimo, o que, em alguns casos, dificulta a navegação pela rede da Internet. “As ferramentas de anonimato barram

qualquer informação, enquanto a máscara filtra, mas deixa passar informações que possam ajudar”, explica Almeida. “Um pouco de exposição é benéfica e contribui para a melhoria dos serviços”, complementa Meira Júnior. “É o caso das empresas de telefonia celular, que monitoram todos os movimentos do telefone, traçam o perfil dos usuários e lançam planos e pacotes promocionais que atendem a maioria dos clientes”, exemplifica. “As compras nas livrarias virtuais também podem ficar mais interessantes se você deixar claro as suas preferências. Os programas instalados no site registram o perfil literário e enviam preciosas dicas aos clientes virtuais”, lembra Almeida, que testou os mecanismos de formulação das máscaras no site de uma livraria eletrônica real.

Mensagens detestáveis - Por outro lado, não faltam motivos para preocupação com a privacidade na internet. “Existem empresas nos Estados Unidos especializadas em capturar dados, traçar perfis, mapeá-los e vendê-los”, conta Almeida. Se hoje as informações são voltadas para o marketing direto que entopem as caixas de mensagens dos “selecionados” com os detestáveis *spams* – e-mails não solicitados e nem autorizados –, nada impede a essas empresas especialistas de rastrear as idas e vindas dos surfistas da Internet que decidam mudar o foco e ultrapassar os limites da publicidade personalizada.

Como na rede é possível coletar dados em quase todas as operações, inclusive nos correios eletrônicos, essas “inocentes” empresas voltadas para o marketing digital podem estender a clientela e passar a vasculhar dados médicos em hospitais ou empresas de seguros saúde para atender a finalidades que os usuários desconhecem. Isso sem falar nos projetos desenvolvidos pelo governo norte-americano que prevêm detectar comportamentos, considerados suspeitos por eles, de pessoas em qualquer lugar do planeta.

Seguro e personalizado - A estrutura de máscaras desenvolvida pelos pesquisadores de Minas Gerais é segura porque gera uma identificação temporária e anônima, que o usuário adota enquanto navega, impossível de ser recuperada pelos sites e outros programas. Um mesmo usuário recebe várias identificações, dependendo dos locais visitados. Ao acessar um site que identifica os visitantes, por exemplo, seus dados estarão totalmente protegidos e apenas a identificação da máscara, que não contém nenhum dado do usuário, será capturada. No entanto, a máscara oferece informações que podem ajudar a personalização dos serviços dos sites.

O sistema é inovador porque seleciona o grau de privacidade. Como esse conceito é, além de cultural, muito pessoal, o próprio internauta decide os dados pessoais que podem circular pela rede. Em linhas gerais, a arquitetura das máscaras funciona com dois recursos: o agente de privacidade e o servidor de máscaras. O agente fica instalado na máquina do usuário e tem a finalidade de negociar com o servidor a máscara mais adequada ao site eventualmente visitado, além de alertar sobre o nível de ameaça à privacidade. O servidor, que pode estar em qualquer lugar da rede, tem a função de armazenar as máscaras e selecioná-las de acordo com o site visitado. Uma caixa de diálogo alerta sobre os dados colhidos pela página acessada na Internet e dá a chance ao usuário de controlar informações que não quer revelar. Em determinadas situações, as máscaras devem ser desativadas. “Nos sites seguros, como os de banco, onde a identificação é fundamental, temos que abrir mão do anonimato para usufruir dos serviços online”, lembra Almeida. ●

O programa
será gratuito
e deverá estar
finalizado até
o final do ano