Impressoras trazem sistema que permite identificação

Foi anunciada, no dia 17 de outubro de 2005, uma descoberta muito importante realizada pela EFF — Electronic Frontier Foundation: diversas impressoras trazem, escondido de seus usuários, um sistema que permite a identificação da impressora e dos papéis por ela impressos. O resultado da pesquisa pode ser encontrado em: http://www.eff.org/Privacy/printers/.

Cabe notar que a EFF é uma das mais conhecidas e respeitadas instituições de defesa da privacidade nos meios eletrônicos, atuando desde 1990. Já publicou diversos estudos sobre proteção da privacidade e direitos civis em todo o mundo. É também a fundação que suporta o sistema de navegação anônima conhecido como Tor (http://tor.eff.org/), que criptografa e oculta os dados de navegação dos usuários.

O título da página já é sugestivo: Is your printer spying on you (Sua impressora está te espionando)? A notícia, que ainda não mereceu o devido destaque, é assustadora. Em resumo, o que se descobriu é que todas as páginas produzidas por diversas impressoras, de vários modelos, imprimem de forma muito camuflada um código que traz informações sobre a máquina utilizada, como seu número de série e a data da impressão. A lista das impressoras nas quais se identificou o código pode ser encontrada em http://www.eff.org/Privacy/printers/list.php. A lista é enorme e inclui impressoras de diversas marcas, como Brother, Epson, HP, Canon, Dell, Lexmark, Xerox, etc.

O texto da EFF é iniciado assim: imagine se todas as páginas que você imprimisse pudessem identificar, com um código secreto, qual foi a impressora e a data da impressão, e, potencialmente, quem a imprimiu?

Devemos notar que as impressoras que utilizam os códigos pontuais de identificação o fazem da forma mais oculta possível. Normalmente, para se encontrar o código, é preciso aumentar a imagem de 10 a 60 vezes e colocá-la sob uma luz azulada para que os pequenos pontos amarelos apareçam. Ou seja, parece claro que a intenção é mesmo de não deixar os usuários perceberem a existência do código. E o pior é que tal sistema foi inserido, ainda segundo o site da EFF, por pressão do governo norte-americano.

A intenção não poderia ser outra: identificar quem está imprimindo textos, mesmo que anônimos. O perigo para os usuários, e para a população em geral, é enorme, e os casos em que isso pode provocar algum tipo de problema são inúmeros, como por exemplo identificar o autor de uma denúncia supostamente anônima, o participante de algum concurso público que exija documentos sem identificação, ou mesmo um documento qualquer, por mais singelo que seja, em que o autor não queira se identificar. Quando uma impressora é vendida, o número de série vai na garantia e na nota-fiscal, tornando simples identificar todos os documentos por ela impressos.

As duas grandes preocupações da EFF são: a) a comprovação da existência de acordos sigilosos entre o governo norte-americano e empresas para facilitar a espionagem e b) o fato de não haver lei que impeça esse tipo de ação nos EUA.

Mas não se pode concordar com a última preocupação da EFF, pelo menos no Brasil. NossaConstituição Federal assim dispõe:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X – são **invioláveis a intimidade, a vida privada**, a honra e a imagem das pessoas, **assegurado o direito a indenização pelo dano material ou moral** decorrente de sua violação;

XIV – é assegurado a todos o acesso à informação e resguardado o **sigilo da fonte**, quando necessário ao exercício profissional;

Ou seja, ou seja, nossa Constituição claramente garante a inviolabilidade da vida privada e da intimidade.

Ora, como não considerar como violação da intimidade e da vida privada a inserção de um código oculto nas páginas impressas, sem o conhecimento do usuário? Como defender que colocar um código de identificação nos papéis enviado a um jornalista por sua fonte, que tem constitucionalmente garantido o direito ao sigilo, não seria violação de nossa norma mais importante? Importantes denúncias anônimas sobre narcotráfico, pedofilia e outros crimes poderiam, a partir de sistemas como o descoberto pela EFF, identificar os autores tanto para a polícia quanto para os próprios criminosos caso estes venham a ter acesso aos documentos impressos.

É certo que nossa Constituição, no mesmo artigo 5º, inciso IV, veda o anonimato (*IV — é livre a manifestação do pensamento, sendo vedado o anonimato*), mas em nenhum momento dá poderes a quem quer que seja para, sem o conhecimento dos afetados, os identificar. Aliás, quando a CF trata da manifestação do pensamento ela faz referência à publicização de idéias, não adentra à esfera privada do inciso X.

E ainda continua nossa legislação, no Código de Defesa do Consumidor (Lei 8.078/90):

*Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e **dados pessoais e de consumo** arquivados sobre ele, bem como sobre as **suas respectivas fontes**.*

§ 1° Os cadastros e **dados de consumidores** devem ser **objetivos, claros, verdadeiros e em linguagem de fácil compreensão**, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2° A abertura de cadastro, ficha, registro e **dados pessoais e de consumo** deverá ser **comunicada por escrito ao consumidor**, quando não solicitada por ele.

Nosso CDC deixa ainda mais claro que não se pode agir dessa forma sorrateira, principalmente quando se trata de relações de consumo, como por exemplo ao se registrar dados pessoais e de consumo, e os abrir para quem quer que seja, sem que os envolvidos sejam informados por escrito de tal fato. Além

disso, é vedada utilização de meios ocultos, que não sejam de fácil compreensão.

Parece claro, portanto, que tal recurso não encontra proteção alguma em nossa legislação; ao contrário, é vedado e pode ensejar até mesmo pedidos de reparação para os consumidores e a tipificação de crime na prática dos fabricantes.

Mas o que parece ser mais perigoso é o fato de se comprovar a existência de códigos ocultos em sistemas informatizados colocados a pedido de governos ou em interesse das próprias empresas. Como ter certeza que as impressoras conectadas em redes não estão enviando mais informações para outros locais? Como acreditar que programas muito mais complexos que os sistemas das impressoras, como editores de texto, de planilhas ou até mesmo sistemas operacionais não fazem coisas semelhantes? Como saber que não há um espião oculto dentro de cada computador, deixando as mais sutis marcas para serem analisadas por aqueles que conhecem o código? Como garantir até mesmo a soberania de um país que pode estar, sem saber, enviando informações sigilosas para outros governos?

E imaginar que os computadores pessoais enviam dados não autorizados para outros locais não se trata de paranóia ou de fomento a teorias da conspiração. É fato já comprovado. Vale recomendar a leitura do artigo “Windows XP mostra em que direção a Microsoft está indo”, de Michael Jennings, utilizado em palestra do Professor Pedro Rezende, em Brasília, no mesmo dia em que o anúncio dos códigos das impressoras era anunciado (Windows XP Shows the Direction Microsoft is Going, disponível em http://metabolik.hacklabs.org/

alephandria/txt/jennings_windowsXP_en.htm).

Segundo o citado artigo, é relativamente simples verificar, com o uso de um firewall, como o Windows XP tenta fazer pelo menos 16 tipos de conexões diferentes — não autorizadas — com os computadores da Microsoft. Alguns dos tipos de conexão puderam ser identificadas, como uma que indica à Microsoft quais DVDs são executados em seu computador (alguém os autorizou a saber quais filmes assiste?) ou outra que permitiria até mesmo o controle remoto da máquina (“Eu, Robô”?); em outros casos, entretanto, não foi possível determinar o motivo da conexão.

As duas únicas formas de se analisar a existência de espiões escondidos nos computadores e periféricos são a engenharia reversa (proibida em diversos países) e a abertura dos códigos dos programas, com liberdade para depuração e recompilação.

A primeira alternativa é praticamente inviável. A quantidade de dados e as possibilidades de ocultação, com criptografia forte por exemplo, aliadas à proibição de sua atividade, seja pelo termo de licenciamento, seja pela legislação, fazem com que essa possibilidade tenha que ser descartada.

A opção restante parece ser a única que efetivamente pode gerar resultados. Dar preferência a softwares com códigos abertos ou livres torna-se mais do que uma questão ideológica ou econômica: passa a ser uma necessidade para quem precisa de segurança e transparência.

Date Created
28/10/2005