

O que é seu é meu

Por Rafael Evangelista

Data de Publicação: 06 de Novembro de 2006

Computação Traiçoeira integra hardware e software e transfere o controle do computador do usuário para o fabricante. Novo Windows deve incluir a tecnologia.

Logo após o 11 de setembro de 2001 o governo de George W. Bush impôs uma escolha difícil aos cidadãos estadunidenses. Para que tivessem sua segurança garantida, deveriam abdicar de algumas de suas liberdades e direitos. O resultado está nas páginas dos jornais de todo mundo: o risco e a sensação de insegurança só cresceram, e a vigilância, os grampos telefônicos e digitais, as prisões ilegais, a tortura e as violações aos direitos humanos agora fazem parte do cotidiano do país.

A premissa de se abdicar da liberdade em nome de uma falsa segurança, que na verdade é sinônimo de controle, tem seu equivalente no mundo da computação. Chama-se Trusted Computing (Computação Confiável) ou Treacherous Computing (Computação Traiçoeira), como preferem Richard Stallman e a Free Software Foundation. De fato, algo que não se pode controlar certamente está mais sujeito a lhe trair, pois sempre pode agir de maneira inesperada. E a Computação Traiçoeira é isso, o controle do computador aliena-se do usuário, ficando a cargo da empresa que o produziu.

Na prática, a Computação Traiçoeira promove uma integração forte entre software e hardware, usando principalmente de chaves criptográficas. Um chip soldado no computador oferece chaves de identificação que são verificadas e validadas por softwares. Estes, por sua vez, autenticam-se entre si, fazendo com que o sistema operacional valide aplicativos e estes validem os arquivos que produzem. Alterações no software ou no hardware podem ser detectadas e informadas a outros, remotamente. Assim, se você está ouvindo um mp3 pirata de uma música do Metallica, por exemplo, (para falar de uma banda muito ciosa dos pagamentos a seus direitos autorais) a Computação Traiçoeira permite que Lars Ulrich delete seu arquivo com apertar de botão.

Uma bela explicação sobre o que, tecnicamente, é a Computação Traiçoeira e quais as suas consequências é o FAQ "'Trusted Computing' Frequently Asked Questions", de Ross Anderson, publicado em <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>. É um documento grande e em inglês, então vale transcrever um trecho:

"TC (sigla para Computação Confiável/Traiçoeira) oferece uma plataforma computacional em que você não pode alterar o software aplicativo, e onde essas aplicações podem comunicar-se com segurança com seus autores e entre si. A motivação original foi o DRM



(Gerenciamento de Direitos Digitais): Disney poderá lhe vender DVDs que serão decodificados e rodarão em uma plataforma TC, mas os quais você não poderá copiar. A indústria da música poderá lhe vender músicas compradas na rede as quais você não poderá compartilhar. Eles poderão lhe vender CDs que você não poderá tocar três vezes, ou só poderá ouvi-los em seu aniversário. Todos os tipos de possibilidades de marketing surgirão".

Uma dessas possibilidades é o aluguel ou venda pré-paga de software e computadores. Se o consumidor mantém seus pagamentos em dia o produto funciona, se não o serviço é cortado automaticamente.

O Brasil já se tornou campo de testes para esse tipo de venda, vide uma experiência da Microsoft em conjunto com o Magazine Luiza (http://www.dicas-l.com.br/zonadecombate/zonadecombate_20060128.php). Quando o programa foi anunciado, em 1995, as empresas se recusaram a dizer se utilizavam recursos de Computação Traíçoeira. Hoje, Microsoft e Magazine Luiza estão sendo chamados a prestar esclarecimentos ao Procon (http://home.londrina.pr.gov.br/news_det.php?id_news=13726) pois o contrato que o cliente-cobaia assina para adquirir o produto diz coisas como: "Independentemente de qualquer outra política de privacidade que acompanhe o PC, estou plenamente ciente de que o Magazine Luiza e a Microsoft farão o rastreamento e manterão registros de meus hábitos de uso do computador e, pelo presente instrumento, dou plena autorização ao Magazine Luiza e à Microsoft para coletar dados sobre mim e meus hábitos de uso do computador e a compartilhá-los com terceiros com relação ao Teste de Mercado".

A Computação Traíçoeira é a infra-estrutura tecnológica perfeita para a expansão dos DRMs. Pela alta integração entre os softwares e o hardware, fica fácil impor uma autenticação remota obrigatória e, se seu aplicativo ou arquivo não estiver autorizado, ele simplesmente não funciona.

Ela deve tornar também a engenharia reversa uma prática inútil. Quando uma empresa esconde as especificações dos arquivos que seu aplicativo produz (um arquivo de texto, por exemplo), as empresas concorrentes tentam entender "na marra" a especificação do arquivo, para que ele possa ser lido por qualquer aplicativo. Se esse arquivo necessariamente precisar ser autenticado para ser lido, não vai bastar entender a especificação, será preciso ter a chave que o fecha.

Muitos podem argumentar que é possível ficar à margem disso tudo, basta não aderir à tecnologia. O problema é que na vida cotidiana nem sempre todas as opções são viáveis. Quanto mais um padrão se espalha, mais difícil é combatê-lo. Quantas vezes não somos obrigados a enviar arquivos em .doc a repartições públicas ou empresas? Será que, no futuro, não seremos obrigados a enviar documentos oficialmente certificados com Computação Traíçoeira?



O que é seu é meu

Muito criticada pela mídia, por consumidores e por entidades que lutam por direitos civis, a Computação Traiçoeira materializada em produtos já mudou muitas vezes de nome. A Microsoft inicialmente procurava implantá-la em seu projeto Palladium, que depois virou o Next-Generation Secure Computing Base. Hoje a equipe do projeto está reunida sob o nome System Integrity Team (http://blogs.msdn.com/si_team/default.aspx). O novo Windows, o Vista, deverá incluir, nas versões mais sofisticadas, um sistema de encriptação de disco chamado BitLocker. O computador terá um chip (TPM, Trusted Platform Module), que validará a integridade do sistema e, em tese, protegerá fortemente os dados e o sistema do usuário. Esses chips já equipam milhares de computadores hoje, principalmente notebooks Toshiba e IBM.

A idéia da Computação Traiçoeira partiu de um conjunto pequeno de gigantes da tecnologia da informação: HP, Compaq, Microsoft, IBM e Intel. Mas hoje integram o Trusted Computing Group mais de 200 empresas, entre elas a AMD, Samsung, Motorola e outras.

O assunto é tecnicamente complexo e, ao sabor da pressão do público, as empresas tem avançado e recuado em suas estratégias. Pela ânsia com que perseguem a iniciativa parece claro que será muito bom para elas. E para os usuários, será seguro deixar a chave do cofre na mão desses sujeitos?

Veja também:

Vídeo explicativo: <http://www.lafkon.net/tc/>

O FAQ da Computação Traiçoeira: <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

Next Generation Secure Computing Base:
http://en.wikipedia.org/wiki/Next-Generation_Secure_Computing_Base

BitLocker: <http://en.wikipedia.org/wiki/Bitlocker>

Versão Original:
http://www.dicas-l.com.br/zonadecombate/zonadecombate_20061106.php

