

Quando a criptografia atrapalha

Por André Fucs, CISSP, <afucs@cfsec.com.br>

IRRESTRITO / PÚBLICA / ORDINÁRIA

Grupo de Restrição: Irrestrito	Emissão: 21.07.2003
Arquivo: YSP_0009	Versão: 22.07.2003

Declaração de exoneração de responsabilidade

Este documento foi publicado pela CFSEC Security Architects com o intuito de fornecer, de forma rápida, informações precisas e atualizadas. A CFSEC Security Architects tentará corrigir qualquer erro que possa estar presente neste documento, tão logo seja avisada.

Entretanto, a CFSEC Security Architects não pode garantir que as informações apresentadas no mesmo estejam corretas.

A CFSEC Security Architects alerta ainda para os seguintes aspectos:

- O material difundido comporta exclusivamente informações de caráter geral, que não pretendem referir a situação específica de um indivíduo ou de uma entidade;
- Este documento pode incluir informações que não devem necessariamente estar completas, ser exaustivas e exatas ou estarem atualizadas;
- Este documento remete para sites externos, sobre os quais a CFSEC Security Architects não tem qualquer controle e relativamente aos quais declina todas as responsabilidades;
- As informações disponíveis neste documento não são pareceres de caráter profissional ou jurídico.

Todas as informações são providas pela CFSEC somente em uma base "no estado". Em nenhum evento a CFSEC será responsável pelos possíveis danos diretos, indiretos, especiais ou de qualquer outro tipo, derivados do uso deste web site, ou de qualquer outro web site que esteja ligado a este, incluindo, sem limitação, qualquer perda de lucros, interrupção de negócios, perda de programas ou outros dados de informação relacionados ao seu sistema, incluindo o caso de que nos seja expressamente informado a possibilidade de tais danos.

CFSEC Security Architects é marca registrada da CFSEC Sistemas Ltda. As demais marcas registradas são respeitadas.

Prefácio

Sobre o autor

André Fucs de Miranda é Diretor de Tecnologia da **CFSEC Security Architects**. *Certified Information Systems Security Professional* pelo ISC2 e participante de diversos congressos e eventos no Brasil e no exterior, participou durante sua carreira de alguns dos mais importantes projetos brasileiros de Segurança da Informação. Membro do Association for Computer Machinery e do Information System Security Association, participa ativamente de diversos debates sobre a Segurança da Informação no Brasil e exterior.

Provavelmente você concorda, a criptografia é uma das formas mais utilizadas para proteger a confidencialidade de suas informações. Mas será que sua solução de criptografia é capaz de garantir confidencialidade sem comprometer a disponibilidade de seus dados?

Há muito anos os princípios da segurança são apresentados como, confidencialidade, integridade e disponibilidade. É com base nesses princípios que surge a maioria das soluções de segurança do mercado. Entretanto nem sempre o fato de adotarmos uma solução de segurança voltada para um desses pilares, nos garante que os outros estejam igualmente garantidos.

No caso da criptografia de dados, duas grandes preocupações existem. A primeira é que ela funcione a contento e que uma mensagem criptografada possa ser decriptografada sem problemas. Em geral isso é garantido pelo próprio algoritmo. Mas levando-se em conta que, de exata, a tecnologia da informação não tem nada, convém sempre considerar a possibilidade de bugs no software ou hardware de criptografia.

Outro fator ainda mais grave, é a possibilidade da criptografia tornar indisponível suas informações gerando transtorno tão grande quanto o vazamento das mesmas. Parece difícil de acontecer mas não é. Tanto pode ocorrer na criptografia simétrica, aquela com senhas tradicionais, quanto na criptografia assimétrica, que emprega chaves públicas, chaves privadas e senhas. Isso ocorre porque após ser criptografada, a informação não deve ser acessível sem a senha, ou no caso da criptografia assimétrica, a chave privada. A perda de senhas e chaves assimétricas constitui portanto, um risco à disponibilidade das informações por elas protegidas.

Até mesmo soluções que usam cartões inteligentes podem sofrer com esse cenário, visto que os mesmos podem sofrer danos ou serem extraviados, comprometendo a disponibilidade das chaves assimétricas neles armazenadas.

Proteger essas senhas e chaves de uma forma com que não se comprometa a disponibilidade das mesmas deve ser portanto uma prioridade para aqueles que enxergam na criptografia uma solução para seu dia-a-dia. As opções para essas cópias de segurança variam de fornecedor para fornecedor e vão desde a anotação das senhas e armazenamento em cofres até o uso de PKIs com "key escrow". Sendo que último é especialmente interessante para empresas preocupadas em conseguir acessar as informações de um funcionário depois que o mesmo se desliga de seu quadro.

As soluções existem, porém é interessante lembrar que o uso de qualquer uma delas implica em novos riscos. No caso de key escrow de chaves

assimétricas por exemplo, existem hoje duas estratégias: uma é a divisão da chave em pedaços menores, que são então distribuídos entre terceiros de confiança. Complexos algoritmos matemáticos garantiriam que sem todas as partes, não seria possível recuperar a chave original.

Outra estratégia, consiste no uso de uma espécie de chave mestra utilizada para criptografar todos os pares de chave dos usuários. Uma vez criptografados com essa chave mestra, os pares são armazenados em um banco de dados de backup.

Além das questões legais que cercam esse assunto, ambas as alternativas apresentam problemas. No primeiro caso, a simples perda de uma das partes da chave poderia impossibilitar a recuperação da mesma. Já no segundo caso, a simples existência de uma chave mestra é um risco significativo. Caso essa chave fosse comprometida, todos os pares de chaves dos usuários estariam comprometidos.

Cabe ao gestor de Segurança da Informação, julgar os riscos que a adoção de uma solução de criptografia pode trazer. É importante que sejam pesadas as necessidades de confidencialidade da informação a ser protegida. Essa informação precisa realmente ser criptografada? É importante também medir os custos que a perda dessa informação pode trazer. Só se investe em segurança se o custo da proteção for inferior ao da ameaça.

Portanto, ao calcular os custos de uma solução de criptografia, lembre-se de não apenas calcular o custo da perda de confidencialidade. Lembre-se também dos custos que a empresa terá para garantir que essa informação confidencial não se torne “segura demais”.