

Criptografia: teoria e prática

Todos sabem que a criptografia promove a segurança. Entenda como e por quê usá-la ao máximo.
por **Marcio Barbado Jr. e Tiago Tognozi**



A criptografia diz respeito ao conjunto de princípios e técnicas utilizados na proteção digital ou mecânica de informações. Utilizadas desde a antiguidade greco-romana, as práticas criptográficas eram inicialmente aplicadas por ferramentas mecânicas muito simples e perspicazes, que ocultavam mensagens legíveis, cifrando-as em formatos incompreensíveis.

Historicamente, quatro grupos de pessoas contribuíram para sua evolução:

- ♦ os militares (o grupo mais importante);
- ♦ os diplomatas;
- ♦ pessoas que gostam de guardar memórias; e
- ♦ os amantes.

Foram os militares que perceberam uma das principais necessidades advindas da adoção de técnicas criptográficas: alternar rápida e eficientemente entre as metodologias utilizadas. Isso porque vislumbravam a possibilidade de seus especialistas serem capturados por inimigos.

Uma macroanálise da criptografia a revela como um conjunto de algoritmos que, bem empregados, beneficiam diversos processos. Assim, este primeiro artigo de uma série sobre criptografia procura apresentar os mais respeitados algoritmos (e pro-

colos) criptográficos da atualidade, bem como sua forma de utilização.

A crescente complexidade dos cálculos envolvidos na criptografia fez com que o advento da computação pudesse explorar tais conceitos com maior eficácia, devido à rapidez com que os computadores processam operações. Hoje, diversos programas comuns, criados para outras finalidades que não a proteção de conteúdo, já apresentam funções criptográficas através das quais o usuário pode encriptar suas informações. No caso das distribuições Linux, os editores de texto *Vi* e *Vim* são dois exemplos.

Tipos de algoritmos

A criptografia possui duas abordagens. Uma, bastante acessível, sustenta-se em leis matemáticas e é conhecida como “criptografia clássica”. A outra, chamada “criptografia quântica”, é estruturada sobre a primeira e, além disso, faz uso de leis da física. Porém, sua adoção ainda enfrenta barreiras, dada a necessidade dos altos investimentos em infraestrutura envolvidos. A abordagem quântica utiliza fótons para gerar chaves inquebráveis, as ditas “chaves quânticas”.

O foco adotado neste artigo é a criptografia clássica, cujos tipos de algoritmo utilizados são:

- ♦ algoritmo de transposição: rearranja a ordem dos caracteres de uma

mensagem. Um exemplo simples é a transformação de “muito obrigado” em “omtui oobdraig”. Para quem gosta de Matemática, é interessante destacar que esta categoria de algoritmo criptográfico é composta por uma função bijetora para efetuar encriptações e sua inversa faz a mensagem voltar à forma original;

- ♦ algoritmo de substituição: substitui caracteres ou grupos de caracteres por outros caracteres ou grupos de caracteres. Um exemplo simples: “muito obrigado” é transformado em “nvjup pcsjhbep”, substituindo cada letra pela próxima na sequência alfabética. Cabe aqui menção à eficácia que alguns algoritmos deste tipo têm demonstrado no combate ao spam, empregados para proteger endereços de e-mail.

Diversas são as maneiras de se empregar produtivamente algumas técnicas criptográficas clássicas por meio de computadores. Pode-se destacar dentre elas o fortalecimento de duas práticas comuns a qualquer usuário ou empresa: o backup e a troca de mensagens eletrônicas.

Entre as organizações que contribuíram para a evolução da criptografia, destacam-se a RSA Security e a BT Counterpane.

Exemplificando de forma tão concreta quanto prosaica, os conceitos criptográficos buscam solucionar problemas universais comuns a duas situações básicas:

1. proteger informações armazenadas e utilizadas sempre pela mesma pessoa ou entidade, e
2. proteger informações trocadas entre duas pessoas (ou entidades) diferentes.

Simetria

Antes de caracterizar rigorosamente esses dois casos, é conveniente registrar o significado da palavra “simetria”.

Simetria, cujo antônimo chama-se assimetria, diz respeito à igualdade de propriedades existente entre dois lados opostos de uma mesma situação. Um exemplo simples e concreto da existência de simetria é a imagem frontal do famoso mausoléu indiano Taj Mahal (figura 1). Nota-se que, imaginando uma linha vertical dividindo a imagem do mausoléu ao meio, é possível identificar características estéticas de uma metade que também estarão presentes — espelhadas no outro lado. Mais do que isso, é possível enxergar que os referidos detalhes correspondentes possuem a mesma distância da linha divisória imaginária.

O contexto abordado neste artigo trata o conceito de simetria aplicando-o às pessoas e serviços que participam do processo criptográfico. Então, voltando às duas situações já destacadas, a proteção de informações para uso próprio é um caso simétrico, já que a pessoa a utilizar um dado arquivo é a mesma que o guardou. Uma situação comum que se enquadra nesse caso é o backup.

O segundo caso — proteção de informações trocadas com outros — é assimétrico, pois envolve dois usuários distintos. O exemplo básico é a troca de e-mails confidenciais.

A solução elementar encontrada para *caso 1* foi chamada de criptografia simétrica, pois a chave que fecha o acesso à informação é a mesma que o abre.

Já para o segundo caso, encontrou-se uma solução na qual a chave de abertura é diferente daquela que fecha o documento e, por isso, tal mecanismo foi chamado assimétrico.

A proposta apresentada neste artigo é de uso simplificado sob qualquer ponto de vista.

Esta primeira parte teórica apresenta uma coletânea de conceitos fundamentais para o devido entendimento dos próximos tutoriais desta série.

Terminologia

Rigorosamente, os sinônimos “encriptar” (com essa nova acepção) e “cifrar” são os termos mais precisos para descrever a transformação de informações úteis em dados enigmáticos não aproveitáveis. Os opostos de “encriptar” e “cifrar” são, respectivamente, “decipitar” e “decifrar” — também sinônimos que denotam a transformação contrária, que faz dados aparentemente sem sentido tornarem-se informações úteis. O termo “criptografar” não estaria errado em qualquer das situações acima; é apenas pouco específico.

A confusão começa com o termo “codificar”, cujo oposto é “decodificar”.

Há um respeitado padrão do governo norte americano, chamado “Federal Standard 1037C”, que é em verdade um glossário de termos utilizados em telecomunicações, e define o termo *encrypt* (“encriptar”) como sinônimo de *encode* (“codificar”):

encrypt: 1. [A] generic term encompassing encipher and encode. [NIS] 2. To convert plain text into unintelligible forms by means of a cryptosystem. Note: The term “encrypt” covers the meanings of “encipher” and “encode.” [JP1]

Contudo, ocorre que, em determinados contextos, existem diferenças entre “encriptar” e “codificar”.

Bits

É comum ouvir de vendedores de equipamentos, especialmente no caso de roteadores sem fio, que a troca de informações proporcionada pelo equipamento é segura, com o único argumento de que utiliza criptografia com 256 bits.

Além de passarem uma ideia equivocada e simplista de ser a crip-



Figura 1 O Taj Mahal é um exemplo de simetria.

tografia fundamentada em potências de 2, esses números que muitos fabricantes vendem como prova de segurança realmente convencem os consumidores.

Cabe a indagação: por qual razão exatamente esses 256 bits devem tranquilizar o usuário?

Inicialmente, tais números são utilizados tanto na criptografia simétrica quanto na assimétrica. Podem referir-se, no caso simétrico, ao tamanho do bloco utilizado no algoritmo conhecido por “cifra de blocos”; e no caso assimétrico, ao tamanho da chave.

Como no roteador sem fio estamos falando em comunicações entre duas ou mais partes diferentes, o tipo de criptografia utilizado é o assimétrico. Provavelmente, os vendedores se referem a um número que especifica tamanhos de chaves utilizadas pelo equipamento.

Cabe salientar o consenso científico de que mesmo as chaves de 512

bits não oferecem segurança. No entanto, se tal valor fosse empregado às chaves utilizadas nas comunicações sem fio, inviabilizaria a comodidade oferecida pelo padrão Wi-Fi, pois tornaria mais lenta a troca de dados.

Portanto, não há razões para tranquilidade ao se adquirir um roteador que empregue chaves de 256 bits.

Algoritmos

Também chamados de cifras, os algoritmos criptográficos são utilizados em criptografia simétrica e assimétrica para fins diversos, e nem sempre estão diretamente ligados a encriptações ou decriptações. Podem servir a outros propósitos, como a geração de pares de chaves, ou ainda para assinaturas digitais.

Criptografia simétrica

Simple e útil, a criptografia simétrica deve cobrir situações nas quais uma só parte esteja envolvida. Por exemplo, a pessoa que encripta (lado que

fecha) é a mesma que decripta (lado que abre). É aí que está a simetria: a mesma pessoa em ambos os lados.

Um caso digno de destaque pela distorção explícita com que trata a criptografia é o Wi-Fi, cuja proteção mais elaborada até o momento, descrita pelo padrão WPA2, utiliza cifras simétricas em comunicações entre dois pontos distintos.

O motivo dessa aberração é o ganho de desempenho proporcionado por algoritmos simétricos.

Algoritmos simétricos

- ♦ AES: Também conhecido como *Rijndael*, AES significa *Advanced Encryption Standard* (padrão de encriptação avançada). O algoritmo é um padrão FIPS resultante de um projeto do NIST, instituto americano de normas tecnológicas. A cifra está presente nos softwares *BitLocker* e *WinZip*, assim como no padrão WPA2 (802.11i para Wi-Fi) e outros;
- ♦ DES: Algoritmo criptográfico criado pela IBM;
- ♦ IDEA: IDEA significa *International Data Encryption Algorithm* ou “algoritmo internacional para encriptação de dados”;
- ♦ Blowfish: Elaborado por Bruce Schneier em 1993, este algoritmo criptográfico leva o nome do peixe que conhecemos por baiacu.

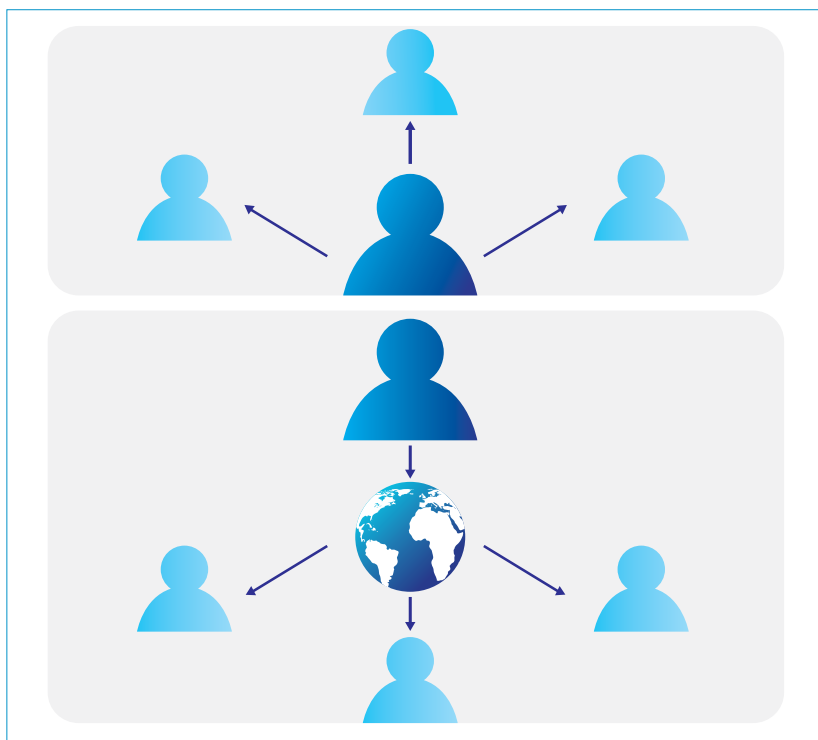


Figura 2 A chave pública pode ser divulgada de duas formas: individualmente, pelo dono, para cada interlocutor, ou do dono para um “servidor de chaves”, que se encarrega de distribuí-la para quem a desejar.

Salt

Recurso poderoso para encriptar conteúdo de texto simples, o *salt* diz respeito a valores pseudoaleatórios concatenados ao texto simples antes deste ser passado a uma função. Os valores e o tamanho do salt podem variar em acordo com a necessidade. Após aplicado à informação, o resultado é entregue à função *KDF* para que o resultado, já considerado protegido, seja então armazenado. O salt utilizado pode ser o IV (vetor de inicialização),

uma sequência de bits necessária para a criptografia simétrica.

Criptografia assimétrica

Herméticas, mas eficazes – e portanto, desejáveis. Assim eram vistas as técnicas assimétricas até pouco tempo atrás. As patentes sobre os principais algoritmos os isolavam do conhecimento público. Tais técnicas, em verdade, ganham projeção ao se considerar a interceptação de informações, um incômodo atemporal.

Pode-se citar 1976 como o ano do nascimento da criptografia assimétrica, pois foi quando Whitfield Diffie e Martin Hellman publicaram o primeiro trabalho descrevendo um sistema assimétrico (então patenteado) nos moldes atuais.

Atualmente, a utilização desregrada de correio eletrônico, alimentada pela sede de produtividade e resultados constitui uma das lacunas mais bem preenchidas pela criptografia assimétrica.

O email desprotegido compromete, mais do que o fechamento de negócios, a vida dos seres humanos por trás dele. Tal conjuntura fez da então hermética criptografia assimétrica uma dribladora das interceptações não autorizadas de dados.

São duas as componentes da segurança proporcionada pela criptografia assimétrica: privacidade e autenticidade, como mostra a **tabela 1**.

As componentes são independentes e podem ser utilizadas separadamente. São úteis, por exemplo, na troca de emails. Porém, tais conceitos são recomendados a qualquer troca de informações entre pessoas ou serviços. Todavia, seu uso exige que cada um dos lados possua um par de chaves, sendo uma chamada “pública” e a outra “privada”.

A chave pública de um usuário de email deve ser do conhecimento das pessoas que lhe desejam enviar

Tabela 1:
Componentes da segurança por criptografia simétrica

Par de chaves	Confere	Importância
Do destinatário	Privacidade	Atribui sigilo às informações trocadas entre partes distintas
Do remetente	Autenticidade	Atribui legitimidade às informações trocadas entre partes distintas

mensagens, e pode até ser disponibilizada publicamente. Já sua chave privada deve ser conhecida exclusivamente pelo próprio dono.

O emprego das duas chaves leva em conta que os interlocutores já possuem, cada um, a chave pública do outro.

Basicamente, caso uma chave pública seja utilizada por um lado, uma chave privada correspondente deverá ser utilizada pelo outro, e vice-versa. Se um lado utilizar uma chave pública para encriptar uma mensagem, o outro lado irá decriptá-la com a chave privada associada. Essa situação utiliza o par de chaves do destinatário.

E caso um lado utilize uma chave privada para encriptar informações, o outro lado irá decriptá-las com a chave pública associada. Essa situação utiliza o par de chaves do remetente.

Chaves públicas são utilizadas no ato de envio, para se restringir o acesso às informações, enquanto que chaves privadas são utilizadas no recebimento – normalmente por uma pessoa diferente do remetente – para obter acesso àquelas informações.

Não é possível a chaves públicas a abertura de informações protegidas, como no exemplo do **quadro 1**.

Chave

Grosso modo, trata-se de uma senha grande: um parâmetro utilizado para se encriptar e decriptar informações. Constituem a menina dos olhos de qualquer criminoso digital profissional, pois, a partir delas, pode-se decifrar dados.

Tamanho da chave

A reflexão sobre a definição deste importante parâmetro, frequentemente dado em bits, causa o que os economistas chamariam de *trade off*, um conflito ou dilema entre dois itens desejáveis, aqui representados por produtividade e segurança. Chaves pequenas (por exemplo, com 512 bits) oferecem melhor desempenho nas operações criptográficas, mas são facilmente quebradas. Em contrapartida, o uso de chaves grandes causa lentidão, mas oferece extrema segurança.

Geralmente, chaves de 1024 bits costumam oferecer um compromis-

Quadro 1: Como uma chave pode ser pública?

Suponha que Dona Flor forneça sua chave pública a Vadinho e a Teodoro; caso Vadinho decida enviar a Dona Flor uma mensagem confidencial, ele utilizará a referida chave que Flor lhe deu para criptografar tal informação.

Suponha que Teodoro, que possui uma chave idêntica à de seu rival, obtenha uma cópia das informações criptografadas enviadas por Vadinho. O primeiro nada pode compreender, pois a referida chave que possui é pública e não serve para revelar informações; apenas Dona Flor, por meio de sua chave privada, tem o poder de decifrar o que Vadinho deseja lhe comunicar.

so interessante entre desempenho e segurança das operações.

Chave privada

Uma chave privada deve sempre ser de conhecimento exclusivo de seu usuário. Apresenta-se como uma senha bem grande em um arquivo texto, com no mínimo 1024 bits, ou seja, uma cadeia extensa de caracteres.

Sendo muito comprida, sua memorização é muito difícil. É exatamente neste ponto que as chaves privadas diferem de senhas tradicionais, pois, ao passo que uma senha pode e deve ser memorizada, chaves privadas devem justamente evitar esse fenômeno.

Por isso, essas chaves devem ser armazenadas digitalmente no computador de seus donos, o que não se aconselha fazer com senhas tradicionais, pois o armazenamento desse tipo de informação em computadores constitui um risco de segurança.

É preciso, portanto, adotar procedimentos adicionais que garantam a

privacidade sobre as chaves privadas de modo a compensar essa vulnerabilidade. Frequentemente, esse problema pode ser resolvido protegendo-se a chave privada com uma senha mais curta e memorizável.

Chave pública

Assim como no caso da chave privada, a apresentação mais simples da pública ocorre por meio de um arquivo texto, como mostra a **listagem 1**. Ela representa a chave pública do coautor do presente texto.

Há muita informação importante entre as linhas:

```
---BEGIN PGP PUBLIC KEY BLOCK---
e
---END PGP PUBLIC KEY BLOCK---
```

incluindo um nome e um endereço eletrônico.

Suponha que Marcio tenha fornecido sua chave pública a todos os

clientes com os quais troca emails. São duas as situações nas quais eles a utilizarão:

- ▶ quando forem encriptar informações que devem ser reveladas apenas a ele (e poderão ser decifradas apenas pela chave privada dele); e
- ▶ quando desejarem verificar a autenticidade da assinatura digital de Marcio (veja a seção “Assinatura digital”) que eventualmente constar em algum email ou arquivo que eles enviar.

Essas situações podem sugerir que uma chave pública é melhor aproveitada quando amplamente divulgada. Isso é verdade em um caso, mas, no outro, requer algum cuidado para que não seja uma mentira. Os dois casos estão respectivamente apresentados na **figura 2**. Note que muitos usuários da criptografia assimétrica utilizam ambos os meios para divulgar suas chaves.

Na **figura 2**, a primeira forma de divulgação é trabalhosa. Requer comunicações individuais com cada um dos contatos e, além disso, exige novos informes sempre que o dono da chave pública precisar se comunicar com um novo contato. É seguro, entretanto, já que os contatos possuem cópias da chave, que receberam diretamente de seu detentor.

A segunda forma parece mais prática, e pode, de fato, ser. Porém, tão prática quanto insegura, caso não se tome algumas providências. O ponto-chave é a confiabilidade das fontes intermediárias, responsáveis por fornecer chaves públicas. Essas fontes representam participantes adicionais no processo de distribuição de chaves. No mais otimista dos cenários, são instâncias adicionais a ser protegidas. Isso consome recursos de diversas naturezas.

Essas instâncias são locais da Internet, chamados de *servidores de*

Listagem 1: Chave pública do autor deste artigo

```
---BEGIN PGP PUBLIC KEY BLOCK---
Version: GnuPG v2.0.11 (GNU/Linux)

mQGiBEkdvc4RBACs31hu82H75EAzMCNehjYtokIqqkH2z1nEw1NDpm8EtjPMQCXw
g+RwLc7VHf+EfwdbC6nYuuI9RLr/Yb92/tmIy8PuhZMpuddBJWW1D0vcKjUpS4j
XHXm3DsF/cax0xBtuUb43myck0rL25ZGQXS1M/ZqtTNR/8PEGZkaD/5KkwCg/FX8
ZWzw3P8uLdRvh/U1DzXN+1cD/3b2vvYvYmhh5Fwd1nASVat0t03DdZ122wH3wJay
2DatAxkLr7bW+hA9PzEIWka3iLNZKnAJcyjj4Dxj9bEU64gtRGEIwDEoG4Cwh9u
K0ooZCJkU9/j2kkU+fbbT0st2H5R8xEWKTOWXy3Lc1zi8bydaAAyvrffjfnxTac
rbEca/93MN6UyNUXXRv+QWD7YqnZSrAcAZaH289imJP7LFrH+8IQQC97MVAKVq
0I8EuFdSN5QAXumvrTCfXwnQ53bLePCz8R9rEuX9zu6oFa2nzCthKoH+kos3fhx9
QxtAQQDYNcJiD/Mq/7t0ntZKmerkxxzfzrScv75rsPQslrrGO+bRCTWfYy21vIEJh
cmJhZG8gSnIgKGJkc2xhYnMuY29tLmJyKSA8bWfY21vLmJhcmJhZG9AYmRzbGFf
cy5jb20uYnI+iFKEEXECABkFAkkdvc4ECwcDAgMVAgMDFgIBA4BAheAAAJE11o
tYNUFxtYY6UAoL9BYLtQnKjp68iWwFpCjLSC7cAEAKDoYLBncdYX9d+7bsMqaMn0
LadXAIhGBBARAgAGBQJKVPfsAAoJEDFGSJKmKWE3rcAn3W5d3JUBv4AVaCVP9Yf
w15x7fDRAU4z3X+S102+FcWqpB91GdSh5FvVnLkBDQRJHbvwEAQA1Lr9rpf7+0VV
1CLkXHzA64T WuohYHvBeiaDErPMqvyPTJvHqiePtt/kHDYjtT/1syaKggkLbXd6
C1xAjkconDVULfiJmniVcEFfKpNzqnfT6tIsggFk/ukakkkS04hbYKBVFM76c
PjnFWBi4Jxv64HmAFy4qc/Zc/DwEcV8AAuUD/AwsG53w0H7p6AybHE/kJ8Xe+5Sx
gltdtGmrI5uE32/hq9qDQ0bK0wEt3QH/QjItzqX31WqEokIID3wEvYJnJmGUVB11
BmEQXDCZ0rWSD8wUHRdiQZfak7xqRyEkMqDqGWTbGVzhBC1ezXSP1KIDeiPy9LY2g
xae1f1bPnPwDURQIEYEGBECAAYFAkkdvc4CAGcKQjW1lg24XG1jAfwCg6GmoeP4W
8gWnLUq8XPxqhsJNohMAni7L132CgFiT3YkiH4rwnSUW2uc
=IdBq
---END PGP PUBLIC KEY BLOCK---
```

chaves, que hospedam chaves públicas gratuitamente. Muitas vezes, facilitam o trabalho de divulgação e disponibilização de chaves às custas da segurança. A chave é disponibilizada uma única vez em um desses servidores, que geralmente é público. Trata-se de uma forma de divulgação que, para aumentar a segurança, exige procedimentos específicos das três partes envolvidas, a saber:

- ▶ o dono da chave pública, que deseja divulgá-la e disponibilizá-la;
- ▶ o responsável pelo servidor de chaves, que será a parte intermediária, e irá abrigar a chave pública; e
- ▶ o contato, também um usuário da criptografia, que precisa obter a chave pública do dono.

Assumindo suas responsabilidades, cada uma dessas três partes pode reduzir os riscos inerentes à segunda forma de divulgação:

- ▶ o dono de uma chave pública, disponibilizando-a em um servidor de chaves, deve se certificar de que o serviço é bem administrado e deve fornecer a seus contatos as informações de acesso a este. Por exemplo, o endereço do servidor;
- ▶ o responsável pelo servidor de chaves deve configurar e administrar corretamente seu serviço, principalmente no que se refere ao cadastro de chaves; e
- ▶ o contato, ao buscar uma chave pública, deve utilizar as informações de acesso fornecidas pelo dono desta, que o conduzirão corretamente ao servidor de chaves.

Contudo, embora esses cuidados sejam simples, eles não são observados e respeitados com frequência. Os riscos, portanto, também são três:

- ▶ caso o dono da chave não assuma suas responsabilidades, obviamente dificultará a ob-

tenção de sua chave pública por seus contatos;

- ▶ se o responsável pelo servidor de chaves não cumprir seu papel, é possível explorar falhas do referido serviço, sendo uma das principais o cadastro de chaves falsas com nomes de pessoas reais (e que, em certos casos, possuem um par de chaves);
- ▶ caso o contato não cumpra seu papel, pode acabar obtendo uma chave falsa que de nada lhe servirá, e ainda prejudicará suas tentativas de se comunicar com o suposto dono da chave.

Percebe-se que o segundo modo de divulgação, assim como o primeiro, exige uma postura ativa do detentor da chave e possui o agravante do intermediário. Portanto, é ilusória a percepção de que um servidor de chaves proporciona praticidade ao usuário.

O ponto que desperta preocupação fica por conta da independência dos servidores de chaves. Mesmo que o detentor da chave pública e seus contatos atuem corretamente, se o

servidor for administrado indevidamente, é possível, por exemplo, que usuários mal intencionados realizem um segundo cadastro do referido detentor, com uma chave pública falsa. Isso confunde os contatos do dono da verdadeira chave e prejudica suas comunicações seguras.

Convém salientar que, ao disponibilizar uma chave pública em um servidor de chaves, muitos poderão obtê-la. Ela poderá ser encontrada por qualquer um com acesso à Internet, mesmo que nenhum contato de seu dono tenha sido notificado sobre sua existência. E isso não constituirá uma vulnerabilidade apenas se os responsáveis pelo servidor possuírem controle sobre o cadastro de chaves.

Um bom exemplo de controle pode ser realizado enviando emails que solicitem confirmação de cadastro. Nesses casos, tais serviços constituem uma facilidade bem vinda.

Uma prova de conceito que demonstra a fragilidade do método de divulgação via servidores de chaves será apresentada no próximo artigo desta série. Até lá! ■

Sobre os autores

Marcio Barbado Jr. (marcio.barbado@bdslabs.com.br) e **Tiago Tognozi** (tiago.tognozi@bdslabs.com.br) são especialistas em segurança na BDS Labs (www.bdslabs.com.br).

Nota de licenciamento

Copyright © 2010 Marcio Barbado Jr. e Tiago Tognozi

É garantida a permissão para copiar, distribuir e modificar este documento sob os termos da Licença de Documentação Livre GNU (GNU Free Documentation License), Versão 1.2 ou qualquer versão posterior publicada pela Free Software Foundation. Uma cópia da licença está disponível em <http://www.gnu.org/licenses/fdl.html>

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site: <http://lnm.com.br/article/3241>