ESTEGANOGRAFIA DIGITAL

Com o advento da Internet, a troca de informações passou a ocorrer com muito mais velocidade e entre muito mais pessoas. Em pouco tempo, esse meio de comunicação se tornou o mais utilizado, não só para a comunicação, troca de conhecimentos e pesquisas, mas também como meio de fornecer serviços que envolvem empresas, governos, etc.

Acontece que a divulgação ou o conhecimento não autorizado de tais informações (muitas das quais sigilosas), pode gerar impactos variados nas organizações, desde problemas financeiros, riscos para o negócio, perda de credibilidade, desgaste da imagem, entre outros.

Esteganografia

A esteganografia consiste em ocultar informação de tal forma que sua existência não seja percebida. Estegano, do grego “steganós”, significa “oculto” ou “misterioso”. Conseqüentemente, “esteganografia” é a escrita em cifra (código), com caracteres convencionais (letras e/ou números) ou especiais (símbolos), de textos. Trata-se de um ramo particular da criptologia que consiste em camuflar uma mensagem, mascarando a sua presença, mas que não torna a mensagem ininteligível.

Ao contrário da criptografia, a esteganografia não pode ser detectada. Arquivos como os de imagem e som possuem áreas de dados que não são usadas ou são pouco significativas. A esteganografia tira proveito disso, trocando essas áreas por informação útil.

Essa técnica não é nova. Relatos da Segunda Guerra Mundial informam que os espiões alemães utilizavam micropontos para fazer com que suas mensagens viajassem discretamente dentro de fotografias. Eram mensagens do tamanho de um ponto (.) que, uma vez as fotos ampliadas, apareciam codificadas para seus destinatários.

Atualmente os hackers e crackers também passaram a inovar nas formas de trocarem informações. Hoje, uma das técnicas mais utilizadas por eles é a esteganografia digital, utilizada para esconder informações em textos, imagens, sons e vídeos, de forma que as mesmas passem desapercebidas aos olhos humanos.

Formas de esteganografia

Como mencionado, a esteganografia é a técnica de esconder um arquivo dentro de outro, de forma criptografada. Por exemplo, colocar um texto criptografado dentro de um arquivo de imagem qualquer. Algumas formas de esteganografia são:

Marcação de caracteres: utilização de uma tinta com composto diferente que ao ser colocada frente à luz faz com que os caracteres fiquem de forma diferente, compondo a mensagem secreta;

Tinta invisível: pode-se utilizar uma tinta invisível para a escrita da mensagem em cima de outra pré-existente, aonde, somente com produtos químicos poderíamos obter o conteúdo.

Bits não significativos: A moderna esteganografia (esteganografia digital) utiliza o uso de bits não significativos que são concatenados a mensagem original e faz uso também de área não usada.

Diferença entre esteganografia e criptografia

Ao contrário da criptografia, que procura esconder a informação da mensagem, a esteganografia consiste em ocultar uma determinada informação, seja um arquivo de texto ou uma imagem, dentro de outro arquivo, de tal maneira que não será possível (de forma normal) perceber a existência dessa informação. Apenas o emissor e o destinatário da imagem “esteganografada” conseguem ver o texto, através do uso de um programa apropriado e de posse da chave usada nesse processo.

Assim, contrariamente à criptografia, que cifra as mensagens de modo a torná-las incompreensíveis, a esteganografia esconde as mensagens através de artifícios, por exemplo, imagens ou um texto que tenha sentido, mas que sirva apenas de suporte. A idéia é mesclar a mensagem numa outra e onde apenas determinadas palavras devem ser lidas para descobrir o texto camuflado.

Já a criptografia é uma técnica que consiste em codificar o conteúdo de uma informação. Neste caso, a informação é enxergada, mas não é possível compreender o seu conteúdo. Para isso, é necessário o uso de um programa específico para criptografia.

Existem duas formas básicas de criptografia: usando uma chave única ou usando uma chave pública e uma chave privada. Chave é uma seqüência de caracteres, símbolos e/ou letras, assim como uma senha. Quando nos referimos à chave única, significa dizer que a mesma chave usada para criptografar uma informação, será também usada na hora de descriptografá-la. Neste caso, torna-se necessário que as partes envolvidas combinem qual será a chave usada nesse processo.

A criptografia baseada em chave pública e chave privada é uma garantia de maior segurança e eficácia na medida em que não há a necessidade de um prévio acordo entre as partes. A chave pública, como o próprio nome diz, é feita para ser divulgada livremente. Esta é a chave que devemos usar para criptografar uma informação. A chave privada é mantida em segredo e usada para descriptografar a mensagem.

Por exemplo, um emissor “A” quer trocar informações criptografadas usando o método de chave pública e privada com o destinatário “B”. Neste caso, “A” deve que codificar a informação usando a chave pública de “B” para que “B”, após receber a informação, possa decodificá-la usando uma chave privada correspondente a sua chave pública.

Esteganografia digital

A esteganografia atual consiste em ocultar informações dentro de arquivos de áudio, vídeo ou imagens e a informação é escondida nos bits menos significativos dos bytes do arquivo. Claro que a mensagem esteganografada só pode ser lida por quem saiba onde ela está e conheça o código para decifrá-la. Aparentemente o que parece uma sujeira ou um ruído no caso dos arquivos de áudio, na verdade, são informações ocultas.

A forma mais comum de esconder informações ainda é através de imagens. Arquivos digitais, de maneira geral, possuem áreas não utilizadas, ocupáveis por informação adicional. Uma imagem é formada por um conjunto de pixels de 8 bits cada um. O pixel é a unidade básica de programação de cor em um display de computador ou em um arquivo de imagem. A cor específica que um pixel descreve é uma mistura dos três componentes do espectro de cores – vermelho, verde e azul.

A idéia é que, alterando-se o bit menos significativo não ocorrem mudanças perceptíveis na imagem. Assim é possível codificar em uma imagem uma seqüência de dígitos binários que contenha um texto usando apenas o bit menos significativo de cada componente (canal) da cor dos pixels.

Aplicações

Uma importante aplicação da esteganografia digital é como “marca d’água”, mensagem oculta de direitos autorais usada juntamente com uma “impressão digital” do produto, número de série ou conjunto de caracteres que autentica uma cópia legítima. A falta da “impressão digital” aponta violação de direito autoral e a ausência da “marca d’água” comprova o fato.

Recentemente a empresa japonesa Fujitsu anunciou o desenvolvimento de uma tecnologia capaz de incorporar dados numéricos de 12 dígitos em imagens impressas em cores, de forma totalmente invisível ao olho humano. Tecnicamente, trata-se de uma espécie de esteganografia e não das técnicas convencionais de incorporação de marcas d’água em imagens digitais.

Tal tecnologia torna possível a inclusão de dados, por exemplo, em anúncios de revistas, nos quais um código de identificação invisível poderá ser lido por telefones celulares ou computadores de mão. Esses códigos consistem de barras pretas e brancas ou pontos geometricamente alinhados que foram projetados para serem lidos por máquinas. Com essa nova tecnologia, os códigos de barra simplesmente “desaparecem” no meio das imagens e ilustrações, ficando invisíveis ao olho humano e os dados incorporados nas imagens podem ser lidos em alta velocidade.

Conclusão

As técnicas de esteganografia digital buscam a ocultação da informação ou, ao reverso, como neutralizar essa possibilidade. Muito do desenvolvimento da esteganografia digital aconteceu em função da necessidade de proteção da propriedade intelectual. Outras áreas de aplicação são a comunicação anônima, comércio eletrônico, sigilo dos sistemas de computação, detecção de informação oculta, urnas eleitorais digitais, privacidade & ocultação de informação e cifragem / decifragem.

Os dois métodos (criptografia e esteganografia) podem ser combinados para aumentar a segurança dos sistemas de informação. Por exemplo, pode-se criptografar uma mensagem e em seguida, utilizar a técnica de esteganografia, trocando-se os bits menos significativos de uma imagem digitalizada pelos bits da mensagem criptografada, e então transmitir a imagem. Se a imagem for interceptada, primeiro será necessário descobrir a mensagem oculta entre os bits da imagem, e, somente após isso, poderá ocorrer a tentativa de descriptografá-la.