Esteganografia

Augusto César Ohashi, Gustavo André Höffling, Serafim Luiz de Alcântara Sobrinho, Walter Ayres, Juliano André Pierobom, Joyce Lustosa e Luis Fernando Martins Garcia.

Universidade Católica de Brasília (UCB) – Brasília – DF - Brasil

augusto@cassi.com.br, gustavoandreh@yahoo.com.br, serafim_ucb@yahoo.com.br, Walter.Carmona@cooperforte.org.br, j.pierobom@terra.com.br, joyce.castmeta@anatel.gov.br, lfernando@anatel.gov.br

Resumo

Com o rápido e crescente avanço de tecnologia de comunicações, formou-se um novo campo de batalha, a internet, onde não existem objetivos concretos, nem se sabe quem realmente é inimigo, muito menos os tipos de armas utilizadas, técnicas aplicadas e o tamanho dos danos que podem ser causados. Por estes motivos, a chamada guerra da informação é o tipo de batalha mais temida atualmente.

Uma das técnicas mais eficazes utilizadas na Guerra da Informação é a esteganografia. Tal técnica consiste na ocultação de informações em diversos meios, como imagens, textos, áudio e vídeo.

A esteganografia pode ser usada para várias razões, como no roubo de dados ou para comunicar uma guerra.

Esteganografia

Summary

With the rapid and extensive growing in communications technology, a new battlefield have been formed, the internet, where there is no real aim and we don't really know who is the enemy, not even which are the kind of weapons used, the techniques applied and the size of a damage that could be caused. By these means, the known "Information War" is the most dreadful battle nowadays.

Introdução

A informação é algo que leva o homem a grandes conquistas, guerras e destruição. Com o advento da internet, a troca de informações se deu de forma mais veloz e em pouco tempo se tornou o meio de comunicação mais utilizado, não só para a própria comunicação ou pesquisas escolares, mas também como meio de fornecer serviços que envolvem investimentos econômicos. A internet, inicialmente, não previa nem seu crescimento estrondoso, nem tão pouco que pudessem aparecer pessoas especializadas em roubar informações e utilizá-las como meio de terrorismo e atentados contra as nações e os seres humanos.

A guerra da informação é uma batalha que amedronta muito as grandes empresas e o próprio governo. Utilizando o roubo ou o uso indevido da informação pode-se destruir grandes negócios em poucos minutos. Os meios e os motivos podem ser a destruição ou apropriação indevida da informação por imperícia de quem a utiliza, insatisfação de funcionários, por um concorrente ou simplesmente por estrelato.

Para não serem descobertos os chamados piratas de computador ou *hackers,* passaram a inovar em suas técnicas nas trocas de informação. Hoje, uma das técnicas mais eficazes se chama esteganografia. Tal técnica utiliza textos, imagens, sons e vídeos para esconder informações de forma que as mesmas passem desapercebidas aos olhos humanos.

Portanto, é de suma importância esclarecer a comunidade a respeito da guerra da informação, dos métodos de troca de informações utilizados na internet, como identificá-los, utilizá-los e, o mais importante, como tentar inibir tais práticas dentro de uma empresa.

Esteganografia

Com o aparecimento e crescimento explosivo da Internet foram criados novos serviços de comunicações, como o correio eletrônico e o uso de servidores WWW. Com tal crescimento, as ameaças ao sigilo das informações também se tornaram mais amplas, fazendo com que a maior parte da comunicação realizada na Internet esteja vulnerável à interceptação, podendo

ter seu conteúdo desvendado com facilidade. Certamente, junto com a criptografia, a esteganografia é uma das maneiras fundamentais para que dados sejam mantidos confidenciais. Ela pode ser usada para manter a confidencialidade da informação valiosa, para proteger os dados de possíveis sabotagens, roubo, ou apenas visualização desautorizada.

Esteganografia é uma palavra de origem grega, onde *Stegano* significa escondido ou secreto e *Grafia* escrita ou desenho. Esteganografia é um ramo particular da criptologia que consiste em camuflar alguma informação, mascarando sua presença. Não se deve confundir criptografia com esteganografia, pois o primeiro esconde o conteúdo de uma mensagem e a existência desta é conhecida, já o segundo esconde a existência da mensagem. Ambas as técnicas podem ser utilizadas em conjunto para se obter um maior grau de segurança da informação.

A esteganografia funciona basicamente com quatro componentes: O **dado embutido** (*embedded data*) é a informação que alguém deseja enviar em segredo. Este dado geralmente fica escondido em uma mensagem aparentemente inocente, chamada de **recipiente** (*container*), que pode ser um arquivo de texto, áudio, vídeo, figuras, por exemplo, BMP, GIF, JPEG, MP3, WAV, AVI ou outros tipos, produzindo um **estego-objeto** (*stego-object*), ou seja, um arquivo com uma mensagem embutida. Uma **estego-key** (*stego-key*) é a chave utilizada para controlar o processo de esconder, assim como, para restringir detecção e/ou recuperação do dado embutido, somente para quem a conhece, ou conheça parte dela. Uma possível fórmula deste processo pode ser representada conforme a figura 2.

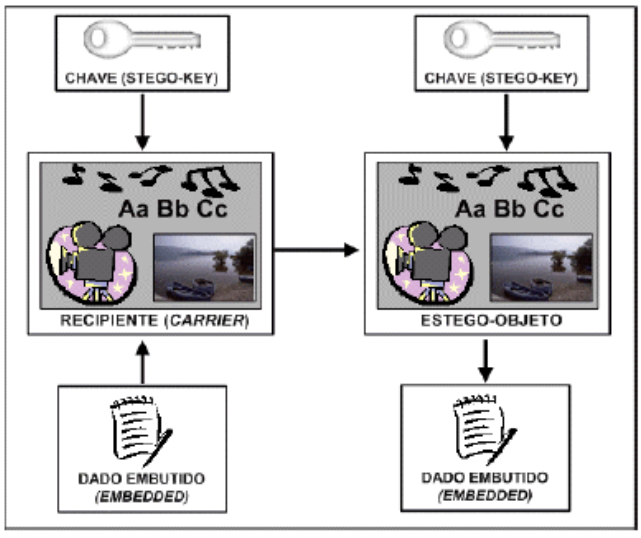

Figura 2 – Terminologia de Esteganografia

Os primeiros registros conhecidos sobre a utilização da esteganografia são datados desde de a.C. 440. Foi largamente utilizada em tempos de guerra. Várias formas de esteganografia também foram utilizadas pelos alemães, como as cifras nulas(mensagem não criptografadas). A invenção alemã dos micropontos foi considerada a obra prima da espionagem, consistia em fotografias no tamanho de um ponto impresso e tendo a clareza de páginas datilografadas em tamanho normal. Em termos de computação a esteganografia evoluiu na prática de esconder uma mensagem dentro de uma maior de tal maneira que uma pessoa não pode discernir a presença ou os indícios da mensagem.

A prática da esteganografia assume que os métodos são de domínio público e a segurança reside na escolha da chave-privada, mas não acontece assim na realidade, os desenvolvedores escondem os cabeçalhos de mecanismos utilizados em suas práticas, justificando a existência da patente.
Alguns softwares de esteganografia utilizam os últimos bits significativos dos pixels da imagem recipiente para adicionar os bits da mensagem. A informação embutida deve ser imperceptível aos sentidos humanos, mas é trivial para que um especialista possa detectar e destruir a mensagem. Outros sistemas assumem que remetente e destinatário compartilham uma chave secreta e usam um gerador de chaves criptográficas. A chave é então utilizada para selecionar pixels ou amostras de som em que os bits do texto cifrado serão embutidos. Contudo, nem todo pixel é apropriado. Alguns sistemas determinam se um pixel candidato pode ser utilizado, pela verificação da variação na luminosidade, nem tão alta como numa fronteira, nem tão baixa como em um campo monocromático. Sempre que um pixel passar por este teste é possível alterar seus últimos bits significativos para embutir um bit de uma mensagem.

Operando técnicas de transformação

O grande problema dos sistemas simples é que, aqueles bits que foram alterados com segurança em um recipiente são redundantes, onde um atacante desavisado sobre a alteração dos bits acredita que os mesmos podem ter sido removidos por um esquema de compressão eficiente. Quando é conhecido previamente o esquema de compressão utilizado, é possível personalizar um método de embutir para obter um resultado razoável. Por

exemplo, em arquivos GIF é possível trocar cores similares, no entanto, se quisermos embutir uma mensagem em um arquivo que pode ser sujeito à compressão JPEG e filtragem, é possível embuti-la em várias localizações.

As técnicas "*spread spectrum*" (espalhamento de espectro) são freqüentemente combinadas às características do recipiente. Por exemplo, um sistema de assinatura de áudio de forma que explore as propriedades de mascaramento do sistema auditivo humano.

Métodos de esteganografia – Imagem

Ferramentas de esteganografia podem ser caracterizadas em dois grupos: *Imagem de Domínio* e *Transformação de Domínio*.

Ferramentas de *Imagem de Domínio* envolvem métodos que aplicam inserção do último bit significativo e manipulação de distorção.

Ferramentas de *Transformação de Domínio* incluem aquelas que envolvem manipulação de algoritmos e transformação de imagens. Estes métodos escondem a mensagem em áreas mais significativas do recipiente e podem manipular as propriedades da imagem, por exemplo, sua luminosidade. Estas técnicas são mais robustas que as técnicas de Imagem de Domínio. Contudo, existe uma relação entre a informação adicionada à imagem e a robustez obtida.

Temos que frizar bem as diferenças entre esteganografia e esteganoanálise. Onde a primeira, esteganografia esconde mensagens secretas dentro de recipientes. Já nas ferramentas de esteganoanálise a idéia é descobrir e tornar inúteis mensagens secretas que estejam ocultas em uma recipiente. Existem várias ferramentas de esteganografia disponível na internet.

Falaremos e teremos como exemplo uma dessas ferramentas gratuitas, que é a S-tools, está ferramenta é utilizada principalmente para esconder textos em imagens. O dado inserido é primeiro criptografado usando passphrase (como se fosse uma senha) e depois com o mesmo passphrase (senha) é usada para gerar uma estego-key.

O S-tools gera um número pseudo-randômico que indicará a posição onde ficará os bits do dado inserido na imagem, vale lembrar que esse número para posição do bit também é criptografado através do passphrase.

Como é feita a inserção dos bits nas imagens? As imagens são compostas por pixels (nada mais é que array de pontos), estes pixels formam a imagem. Dentro do windows por exemplo às imagens são formadas pela junção das cores primárias, vermelho, verde e azul, que são representadas por valores binários, ou hexadecimais. Indo de 0,0,0 que é a cor preta até 255,255,255 que é Branco. Com isso temos uma série de variações de cores que não são perceptíveis por nos.

Por exemplo, suponha que uma amostra de texto será inserida em uma imagem, e onde está pintado de vermelho seja a posição de inserção deste texto.

10111 – 11011 – 11100 – 10101 – 10000

Agora suponha que teremos que inserir nessa imagem um texto onde o binário deste texto seja escrito 01010.

10110 – 11011 – 11100 – 10101 - 10000

Podemos notar que após os dados já inseridos apenas foi modificado o primeiro bloco binário, fazendo com que a alteração fique de difícil percepção humana.

Conclusão

Diante da guerra da informação, não se sabe até que ponto é possível confiar em qualquer informação digital, até porque uma mensagem aparentemente inocente pode estar escondendo informações ou comandos de guerra/terrorismo.

É preciso ponderar que armas de guerra da informação podem ser utilizadas tanto como defesa, quanto ataque.

Todas as formas de se preservar devem ser consideradas, pois sempre haverá alguém com tempo e talento suficiente para conseguir transpô-las. Contudo é necessário muita tática de defesa, obrigatoriamente contra os ataques mais conhecidos, mas também é imprescindível estudar e entender

outras tecnologias, como a esteganografia, que desde antes de Cristo é utilizada, mas que quase ninguém conhece sua forma digital.