Unmasking the Spoof

Another critical security concern that has puzzled and agitated millions of internet users around the world is Spoofing - a form of online deception that incorporates data-packet modification or man-in-the-middle attacks to intercept information between two parties.

It is common knowledge that information travel from one point to another, using online fragmented mediums called packets. These packets often move from secure and unsecured locations. And more often than not, packets get lost along the way, or in more serious situations, get infiltrated by crackers, or web thieves.

Man-in-the-middle attacks are often regarded the more technical of the various spoofing methods, since it requires a working knowledge of various internet protocols, ports and software.

Imagine yourself chatting with someone and pouring much information about your life and your work. While at the other end of the line, your good friend happily responds to your messages.

And in between the two of you, a malicious cracker is taking a laugh, at peeping through your conversation, or in more cases than one, modifying the messages into more private discussions, that benefits only the cracker.

CellHUT.com
82 School Street,
Glen Cove, NY, 11542
Phone: 1-516-583-5110
Fax: 1-646-349-5523

Another type is the URL spoofing or more commonly known as Phishing. One popular website can expect visitors ranging from hundreds to millions per day.

That means, millions of information waiting to be intercepted. Crackers often take advantage of the several key vulnerabilities in the internet to create a sort of temporary loop hole in the packets that users send and receive from websites, masking their own made website, into the appearance of the one that users are currently visiting, and taking advantage of the disguise to steal important information.

Information online is never 100% secure, and is always one way or another, vulnerable to being accessed by someone who possesses the tools and the right technical-background on the type of system that a particular group of people use.

Security providers often suggest the use of certain levels of encryption on private files or data being shared on the internet. While this can greatly help, it is not a perfect solution to data-spoofing.

Users must take it upon themselves to practice some sort of security measure, to ensure that their computers are free from prying eyes.

One sure method which I would like to share is by filtering downloads on your computer. Users often love to download practically everything they see or like on the internet. Some of these files might contain malicious codes, which could help crackers take information from your computers.

So, if I were you, I'd keep an extra vigilant eye over what is downloaded into your computer. You never know, what bug would hit you.