Shareware and Its Network Security

The creation of the concept sharewares was one of the most revolutionary innovations of the 1980's. This new idea allowed the development of an online community of program users that do not need to rely on just retailers. A Shareware is a method of software distribution that distributes softwares for free to download and use. Shareware programs usually are programs one may buy from any computer store, but comes with the advantage of being able to try it out before actually buying it. However, this software is not the full package and comes with basic limitations. Sharewares may comprise of many kinds of softwares that involves: games, software, word processing, real estate, personal finance, etc.

The concept of shareware was originally started in 1982 coined as the term "freeware". It was developed by two programmers named Andrew Fluegleman and Jim Knopf who in fact invented this method from soft ware piracy. The irony was that they used to work for IBM and instead of going through the time to attempt to retail their programs; they distributed their programs in a network that allowed the programs to be copied and further distributed with a request that they receive payments for further developments. Thus, the name *freeware* came to be based on the concept of freely sharing the programs through the internet. When Jim Knopf created his program and started the shareware, the programs ran just within the colleague circle, but soon it expanded and the need to monitor the network created arose. Jim Knopf therefore used a database to monitor all users and he attached notes to his downloads to send money voluntarily as the managing of such a big network and programs become more time consuming. The need for software "piracy" arose, except for in this case the author – Jim Knopf – encouraged the copying of his programs, which actually bought him new business as the consumers were more eager to pay for a "service" that was cheaper than go to stores and may hefty sums to buy software they quite possibly have never used. Thus the concept of shareware was created.

Sharewares are more easily available and cheaper than buying from retail. The greatest advantage of a shareware is that one may use the software for a while and if they don't like it, he or she may simply delete it and not have to pay for it if the software was to be bought from a retail store. Shareware programs are very broad and encompass many types of programs that are useful to the casual gamer to the busiest businessman. However, with the busier traffic and ever expanding internet, the issue of security is increasing.

To learn more about the security protocols and flaws of the shareware networking, one must learn about the general operation of the internet and its networking facilities. The internet is fundamentally a vast network of networks. A computer network is a connection of many computers through land or wireless means. An internet is a vast network that is hosted by many servers that host many other local networks all through wireless means. The computers are hosted through the Internet Protocol or the IP address that specifies a computer's network address to which it is accessed to by other computers or networks. Another computer may be accessed easily if handled by an experienced user or professional. This is a major security flaw in any network system as one may hack into another system without much difficulty. Programmers may easily create softwares that

By: Tahmid Zaman
424350

can hack into other computers through "backdoors" and the IP. This directly leads to and is connected to shareware networks.

http://computer.howstuffworks.com/internet-infrastructure.htm
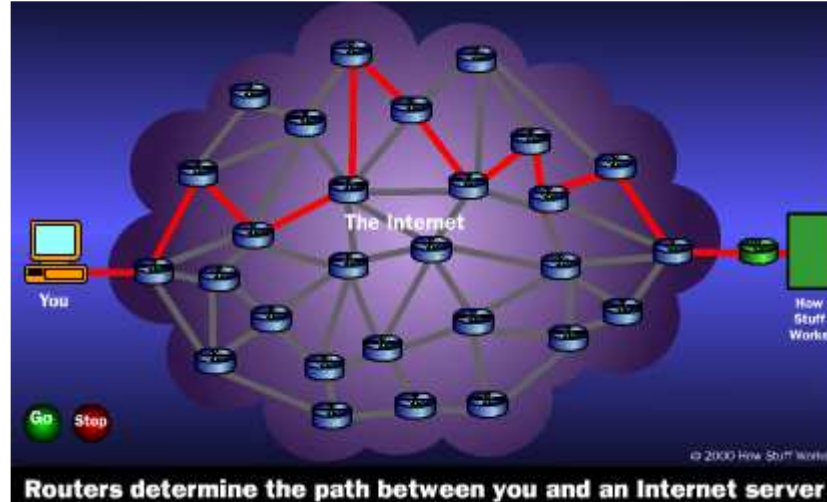
A shareware network is created by the author as the host of the network. In other words, like Jim Knopf, the author may keep track and have a database of all users and their respective IP addresses.
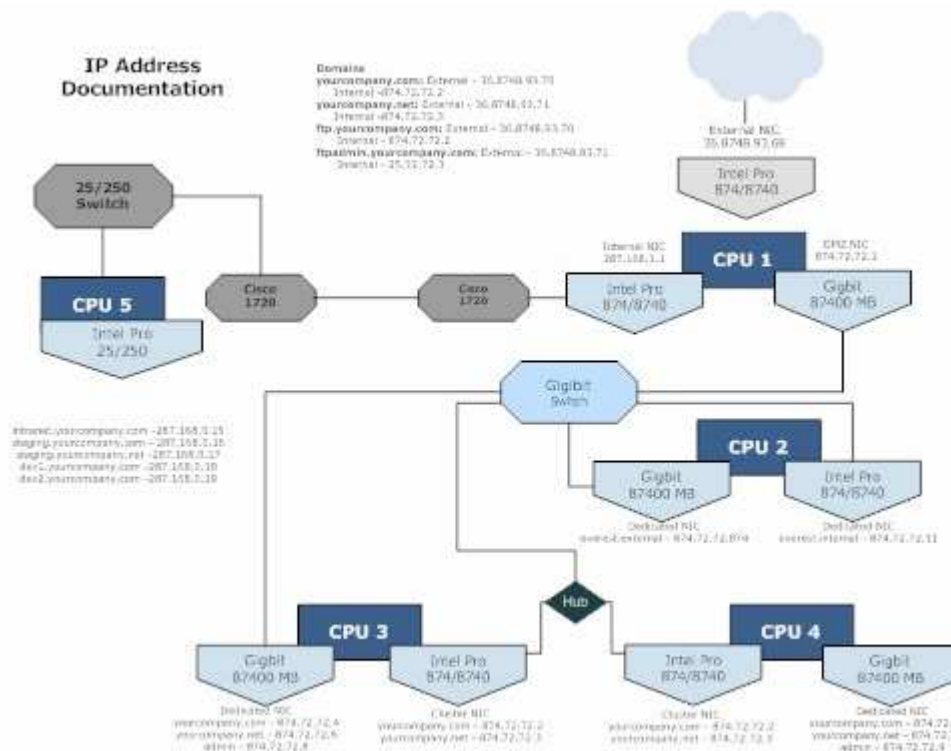
http://www.smartdraw.com/examples/preview/index.aspx?example=IP_Address_Layout_-_01

In a shareware network, the author may allow the uploading and downloading of files unanimously by general users and never actually ensure any kind of protection that the programs, documents or any files are legitimate secure files. This allows some users

By: Tahmid Zaman
424350

to upload Botnets and programs such as Sub7's masked under harmless files and this allows them access to one's computer. A Sub7 is a popular backdoor program that allows users to cause from mischief to crime on other computers through simple manipulation of files to uploading and downloading illegal files such as pornography or credit card stealing. Even though most operating systems are equipped with firewalls and anti-virus protections, any executable files containing this file may establish the connection. This directly correlates with sharewares as the uploaded files may contain such files and may lead to the loss of personal valuables.

Shareware authors themselves may be involved in such misdemeanors as they might create a network and run Botnets that are like an army of independent programs that install themselves into other computers en masse and using the victimized computers to do the Botnet author's bidding. This is highly prevalent in any p2p sharing softwares where downloading and uploading is free and unsuspecting users fall victim to them. These can also be run into any networks like shareware networks that may be created by a criminal to steal credit card or to advertise spam.

Although sharewares have been very revolutionary to the computer world as they allow quicker solutions to frequent and active users, they also come with the price of the same network security flaws as that of any unsecured networks over the internet. The hundreds of millions of people who use the internet on a regular basis are more often than not unaware of such dangers hidden. One may consider the dangers of only "the computer got hacked," but the implications are far more meaningful as faceless criminal lurk every corner of the cyber world without traces and may prey upon an innocent victim not only steal personal information, but also they may target a business and thieve millions of dollars to the unsuspecting. One must always be aware of the existence of such issues and be careful when using sharewares and especially its network, because the author or any experienced user is a potential hacker.

By: Tahmid Zaman
424350

Bibliography

Knopf, Jim. "The Origin of Shareware." Association of Shareware Professionals. 1995.
    Association of Shareware Professionals. 25 Mar. 2007 <http://www.asp-
    shareware.org/users/history-of-shareware.asp>.

Tyson, Jeff. "How Internet Infrastructure Works." HowStuffWorks. HowStuffWorks. 26
    Mar. 2007 <http://computer.howstuffworks.com/internet-infrastructure.htm>.

Author, Unknown. "Sub7." Answers.Com. Answers.com. 27 Mar. 2007
    <http://www.answers.com/topic/sub7>.

Author, Unknown. "Network Design." Smartdraw.Com. Smart Draw. 27 Mar. 2007
    <http://www.smartdraw.com/examples/preview/index.aspx?example=IP_Address_La
    yout_-_01>.

Bradley, Tom. "Computer Security 101 (Tm)." About.Com. Fortune 100 Firm. 27 Mar.
    2007 <http://netsecurity.about.com/cs/compsecurity101/a/aa112903.htm>.

Author, Unknown. "Botnet." Answers.Com. Answers.com. 27 Mar. 2007
<http://www.answers.com/topic/botnet>.

By: Tahmid Zaman
424350