Sergey Purkar
A.V. Gerasina, research supervisor
V.V. Gubkina, language adviser
SHEI "National Mining University", Dnipropetrovsk

Hacking: Problems and Solutions

The biggest problem information systems facing is hacking. Hacking takes place when an illegal user tries to access private information without having authorisation. This illegal access is done either by using Trojan horses, logic bombs, and many other types of software that can be very easily hidden. Sometimes the hackers will even go as far as crashing an entire network. The repercussions from the attack of hackers can do serious harm to business. Hacking is still remained a hot topic for the government offices.

Nowadays administrators or end users can take some preventative measures. Firewall is considered to be the most commonly used preventative measure. It is a program used to protect computer from outsider attacks. In addition there are some other programs to be set for preventing information from hacking.

The solution to deal with these "cyber vandals", however, has been primarily found in the form of new legislation. There is a great plenty of laws aimed to cope with different types of hacking. Unfortunately, there can be no true solution because as innovative as programmers become hackers will match their innovations and skill. The key to controlling this issue is to stay one step ahead of these hackers and continually develop new and better forms of protection.

The best way to stop someone from hacking your computer is to have a Firewall installed. HowStuffWorks.com says "A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through." Essentially, a firewall is a blockade to keep harmful forces away from your computer and personal information. There are three ways that a firewall can control traffic in and out of a network: Packet filtering, proxy server, and Stateful inspection. Packet filtering is analyzing small pieces of information against filters. If the information does not make it through the filter then it is thrown out. Proxy server is when the firewall finds the information you need on the Internet so that you are sure that the information is secure.

HowStuffWorks.com states that Stateful inspection is "a newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information travelling from inside the firewall to the outside is monitored for specific defining characteristics, and then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded." (http://computer.howstuffworks.com/firewall1.htm)