The Beginning Of An Evil

The net did not exist yet. Hackers were mainframe programmers, Commodore 64, and Apple users. Cracked software and hacker/cracker tools are traded between friends. Joe trades his "cracked" (copy protection removed) of a hot new game to Pete for Pete's home brew disk editor. There were ethical standards imposed upon these trades and hackers who demonstrated anti-social behaviour where soon ostracised and no longer traded with. This kept things under control to a great extent. Most hacked for the knowledge foremost with the challenge and the competition running close behind. Who can break the new game first? Who can write the best tool? Groups formed, combined their efforts, and tried to outdo each other.

The IBM PC is released and computers and software become more plentiful, cheaper, and a lot more people get into hacking.
The software companies begin to use more and more sophisticated security measures to prevent their software from being copied. The hackers became better and better and breaking them. It becomes the great game! The hackers are generally respected among

other programmers; their skills admired. Being a hacker was a good thing.

The BBS age - The modem came into wide spread use. Soon BBS's (Bulletin Board Systems) sprang up all over the place. These were computers with one or more modems attached to them. You could connect with other users of the BBS here. You could chat, download files, send mail, and post messages on these systems. Now all kinds of software and images where able to be traded. But trading was now different, for every file you uploaded you could download 10! This speeded up the distribution of the hacking tools, and removed most of the peer pressure that had kept things under control before.

The modern hacker is born. The BBS's also gave hackers a new challenge, that of hacking into another system remotely. Hacking into the BBS' computers becomes the new thing to do.

The malicious hacker is born. It also gives rise to the bad boys. They are the ones that when thrown off the BBS for anti-social behaviour, they strike back by hacking in and defacing the site and destroying files. Security measures start to be implemented to combat this.

The second round begins. Now it is the hackers vs. the security systems. The game continues....

Many corporations and universities now have computers. Most of these have modems installed, mainly for the manufacturer to perform remote maintenance. Now hackers are breaking into these computers as well. Hacking becomes a much more serious threat. At this time there is very little in the way of security systems in place to prevent the hackers from getting in, the BBS's are way ahead of the corporations in this area. The break-ins, when they are noticed, get very little publicity.

Hidden away in the university labs, the net is being born. Only a few computers hooked together at first, but it begins to grow rapidly. The modern hacking tool is born. Hackers start creating new tools. One of the important ones was the dialler. A dialler is a program that dials all the numbers in an area and finds the modems there. The better ones would even test for known logins and passwords.

The movie "War Games" comes out. The world now knows the word "hacker". Hackers are now either considered dangerous nuts, or

modern heroes. Suddenly lots of teens want to become hackers. "Hacker" BBS's proliferates. Diallers and other tools proliferate as well. Some of these new hackers make mistakes, accidents happen. More anti-social types join in, and the malicious hackers delete files, crash systems, and generally wreak havoc. The sysops begin to realise that all is not well, and security awareness begins to rise, but most are not nearly as skilled as the hackers are.

Blue boxes. Blue Boxes ("free" long distance) and dialler software merge and hackers begin to use the phone system to spread beyond their local area. The Phone Company starts going after the hackers for illegal use of the phones. Laws are starting to be created concerning computer crime, but they are feeble and vague, but before this time all the hacker activity was not violating any laws except perhaps for some copyright infringement.

The Net age - The net now includes 100's of computers. While there are no ISP's, many universities, and corporations where now linked together. These computers have modems, so hackers start visiting other systems using their local hacked system. The

shell account is born. Hackers use PC's and modems to break into local systems, give themselves a full access account, and use it the break into other systems in the net. As the net grows and the number of hackers grows with it, more accidents happen, and malicious hackers delete files, crash systems, and generally wreak havoc.

The Web Age With the domain name system in place the World Wide Web is born. There is an explosion of computer users going on-line. The BBS's quickly move to the web, and now the tools and tricks get very widespread distribution.

Windows and GUI interfaces take over, and we now have point and click hacking. This leads to a new kind of hacker, called "script kiddies". The script kiddies have very low skills, but they don't need skills with the new tools. This new web also makes everyone anonymous.

This anonymity makes the kiddies bold, and they feel they can do anything with no repercussions. This sets off a wave of anti-social behaviour that rocks the net. Viruses, Trojan horses, DOS attacks. Malicious hacking becomes the norm and the old style curious

hacker becomes a vanishing breed. Security becomes a major issue, but for every security hole plugged, two new ones open up. Shell accounts become even more important now, and hiding your tracks becomes both easier, and more important. Laws are passed and the FBI and SS get into the act.

So far law enforcement has had little effect. They can only catch the real losers, those who are too ignorant or stupid to cover their tracks. The good ones, the informed ones, make their attacks with impunity, and even when detected the attacks mostly going unreported for fear of bad publicity.

The Elite hackers have even more power now, their knowledge and skills are much better than the average Sysop, and the Elite can pretty much do as they please. Most of the ethical ones are lured by big money to work for the "other side" and become network security experts.

The unethical Elite hackers become a true criminal element in hacker scene. Now we have KGB trained cyberspys, credit card number thieves, and the information thieves stealing corporate secrets among others.

Internet Security

It was in the news lately that US Soldiers searching a Taliban flea pit in Afghanistan discovered instructions on how to build Nuclear Bomb. There was all out panic, how could they have got such "classified information"? Could it be from Iraq? Russia? Cuba? Or from a source available from most homes and buildings around the world?

The Internet is a source of information with no control. Yes there is, I hear you cry. There are firewalls, and filters like Novell and Net Nanny but to someone who wants to find something they are 0% effective.

Within a few clicks I myself had pulled up these "classified instructions" on how to build a Nuclear Bomb. Also freely available are instructions on how to make a variety of home-made weapons and explosive devices. Such instructions are found in documents like "The Terrorists Handbook" and "The Jolly Rogers Cookbook".

All these tools of evil are placed on the Internet by hackers and so called anarchists.

These people are nothing but social outcasts and the destructors of a civilised way of life. What do our governments and police forces do to track down these wrong doers and remove this filth form the reaches of people we would rather not have the information? Nothing!

Over the past ten years the US government has spent more money chasing down Bill Gates, founder and owner of Microsoft who without we would be with poor computers, than evil doers like Saddam Hussein and Osama Bin Laden.

More has to be done to remove these sources of information form the Internet if further terrorist attacks are to be prevented. What if a child got hold of the information and for a “laugh” decided to blow up grandma’s cat with a blast bomb. Not only would it result in the un-needed death of a small animal but also the child could be seriously maimed or even worse killed.

To prevent further terrorist attacks first of all we have to conquer the biggest terrorist of all “The Internet Terrorist”.

This is the real “new war” which governments around the globe are trying to combat. The FBI

(the worlds most useless secret service) have their own anti hacker divisions which are mainly composed of the very people that they are trying to catch. It's ironic how the powers that be use the powers of the underlings to remove themselves of what they tend to call "earth's unwanted beings".

It seems as well that teenagers, most of them being teenage boys, are fascinated by hacker "promoting" movies like The Matrix, Hackers, Swordfish and The Lawnmower Man. This is another cause for there being so many new Internet related crimes. It is seen as cool to break into other computers and steal their well-valued data. It is seen as a fun and un-dangerous thing to do, as most times in films these people never get caught. The reality of this is far more shocking and real. The way we could work around this new and on going problem would be to have a lot stricter censorship on films and on the media itself. Neutralise the poison at the bite.

To stop the "professionals" tying to access your computer you could invest in a firewall. These are complicated things (why is it that people insist in complicating what could be very simple?) which sit in your Internet provider's computer. You have no control

whatsoever over them. These firewalls are only as good as the people who maintain them. These also have holes in their workings which people can crawl through which makes them utterly useless.

Anti virus software is a useful weapon in the war. A vaccination for nearly every virus is available but with new virus on the go everyday the pharmacy of anti virus software runs dry.

Yes they can filter the Internet. They could close down one of the thousands of websites but for everyone they close down another five would pop up. The only way they could completely destroy the world of the Internet Terrorist would be removing his only source of life, the Internet itself. But why should the enjoyment of millions be sacrificed for the malicious use of the few. This is a war, which will go on for as long as time itself does. Man against man using computer against computer. This is the war of the Internet.