

# Internet Ready Is It Really? First internal draft

Arron Martin Zeus Brown,  
University of Teeside  
SSTUK

February 12, 2007

## 1 Introduction

This paper came about due to some observation, the first being the growing trend in new and inexperienced people buy home computers only to find out that they have fallen victim to some sort of internet crime. The second observation and the probable cause for the first observation is the so called internet ready computers being sold in many computers store often by staff that are poorly trained in computer security, while it is unfeasible to expect sales to be computer experts of any type, surely it is feasible that so called "internet ready computers" should be just that.

In most case these so called "internet ready computer" are far from that, in some case the term is being used to state that the system has a modem of some sort install, however this paper will look at the problems caused by this trend and what can be done to counter act this and make "internet ready computers" just that.

### 1.1 why do people want to go on the internet?

Millions of people use the internet and each person will have there own wants and needs. They can include thing such as education, entertainment employment and socialising but there are some people that have learnt that the

internet can be easy pickings for them to find victims, these so called cyber criminals and the public often cross paths in any of the zones in (ref fig 1). These are by no means the only arena for the crimes to place in. to ask some one to police them is at this time unfeasible as time, technology and money restricts this possibility this means that the internet can be an unsafe place.

However if all user's really did have internet ready computers this ability to commit these crimes would be limited, in section 2 this paper looks at some of the problems unsecured computers connected to the internet and why there is a need to address this issue.

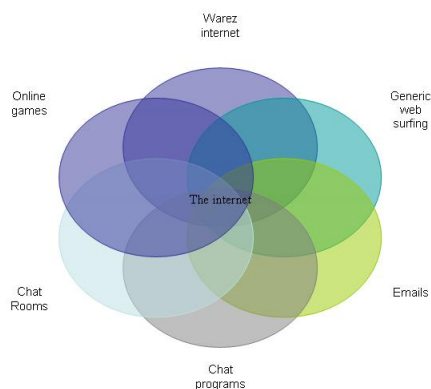


Figure 1: internet zones

## 2 Why worry

So why should we be concerned about these systems and the affect they are having on the internet if are system are secured. Well one easy to point out reason would be The DDOS (Distributed Denial Of Service), it is the unsecured system that are becoming the reflection servers communing know as Zombie systems (ref fig2) there for these "internet ready" systems can and are affecting most internet user in some form or another. It can be seen in internet crime figures and server disruption around the time's when computer are purchased in mass such as Christmas and the start of the new educational year. The DDOS is just one type of attack the following section 3 to 5 explain some more attack types that "internet ready" system and why

they work. The paper will then look at what is needed to be really internet ready (see 6), then the paper will discuss some possible solutions (see 7)

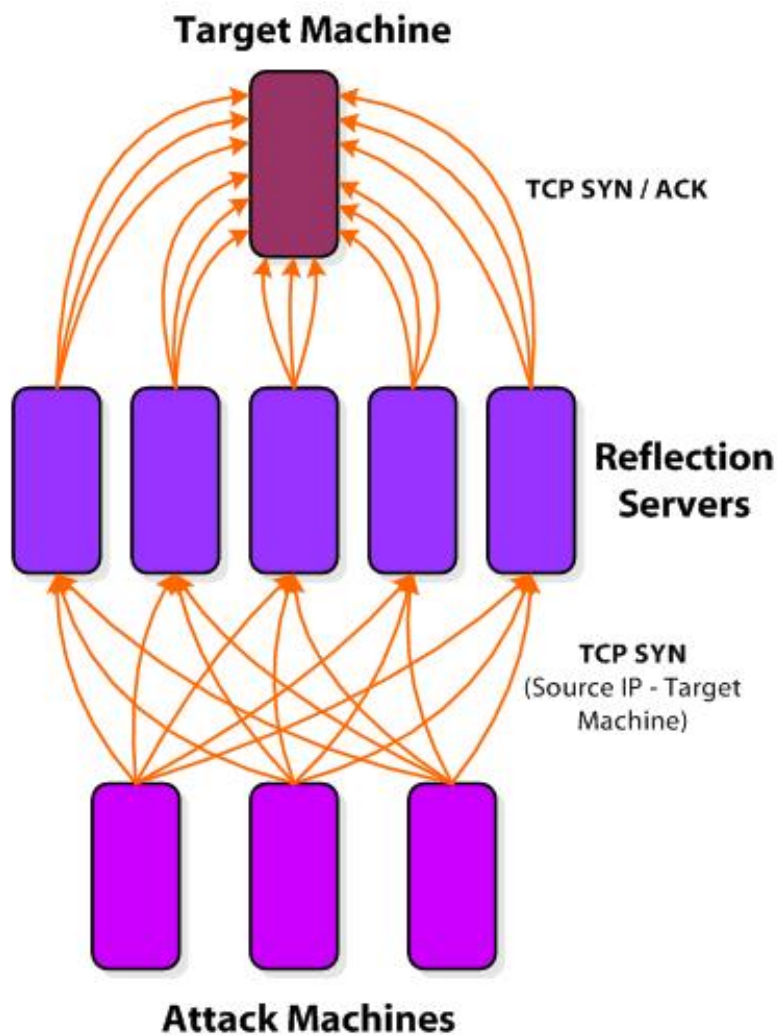


Figure 2: Simple DDOS Attack

### 3 Computer Crime

So the first thing we should do is state what we are classing as the crimes that this "internet ready" type system may be involved in. If we look at

The Computer Misuse Act, 1990 it gives us a board outline of any computer related crime

1. Unauthorised access to computer material. Described as simple hacking - that is, using a computer without permission. This now carries a penalty of up to six months in prison or a 2000 fine, and is tried in a Magistrate's Court
2. Unauthorised access to computer material with the intent to commit or facilitate the commission of further offences. This section of the Act covers actions such as attempting to use the contents of an email message for blackmail. This is viewed as a more serious offence; the penalty is up to five years' imprisonment and an unlimited fine
3. Unauthorised modification of computer material. This section of the Act covers distributing a computer virus, or malicious deletion of files, as well as direct actions such as altering an account to obtain fraudulent credit

The later two offences are tried before a jury. The act also includes the offence of conspiracy to commit and incitement to commit the three main offences. This aspect of the Act makes even discussion of specific actions, which are in breach of the main sections, questionable practice. It is sufficient to be associated with an offender in planning the action, or to suggest carrying out an action which is illegal under the Act, to be in a position to be charged.[3]

How for the preposess of this paper we must define what computer crime is and what internet crime is see sections 3.1 and 3.2

### **3.1 What is Computer crime?**

This criminal activity takes place in the real world, the criminal act must not be committable with out the use of a computer or electronic device, for instance the pirating of computer software and producing CD/DVD burnt with the copy write. However the above example could then be looked at not as computer crime but as a computer aided crime, as the crime here is Copy-Write theft and this crime can be carried out with other products without the need for computer.

To be a true computer crime the crime must be only committable by using a computer for instance the act of virus creation for the purposes of malice

acts is now classed as a computer crime in many countries with in Europe and the United States. This crime can be classed as a computer crime; some people here may think that it surely falls into internet crime. However they would be wrong as it is not the distribution method of the virus that is the crime, and the virus could be distributed on CD/DVD or floppy disc.

### 3.2 What is Internet Crime?

As the computer crime showed, internet crime also has two levels the first being internet or network aided crime, and the second being a crime that is only committable via the use of the internet. In today's world there are many examples of internet aided crime, these range from the distribution of files, these can be any form of illicit material to virus propagation.

However internet crime is much less of a problem as there is still very few crimes that are committed on a network such as the internet that can only be committed on the internet. One of the problems that has been highlighted by the media, is the use of chat rooms as a grooming tool with the intention to commit some sort of paedophilia crime. The true grouping therefore must be listed as : None technology aided crime. Technology based crimes and its

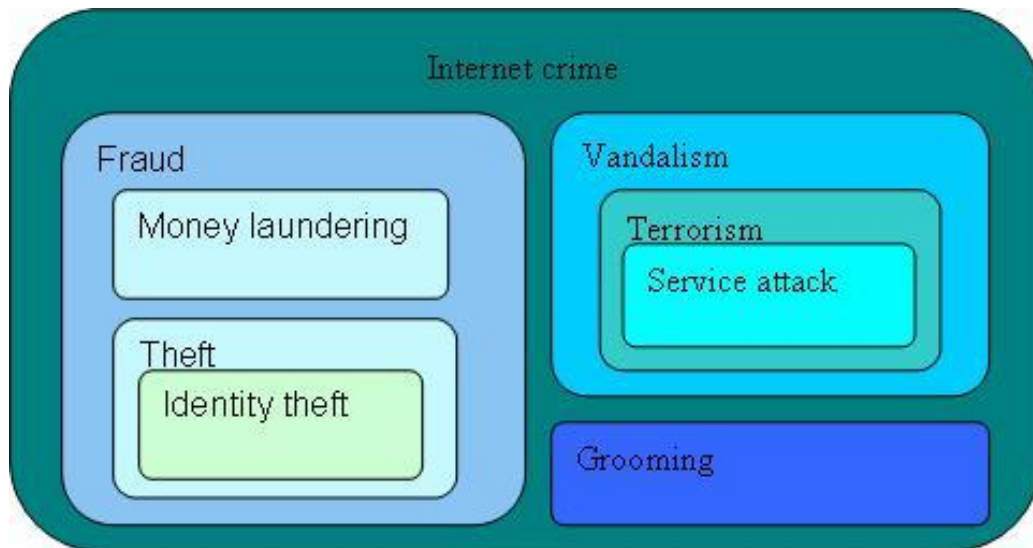


Figure 3: Internet Related Crime Map

four categories.

1. Computer aided crime.
2. Computer crime.
3. Network aided crime.
4. Network crime.

## **4 The Threats To Home Users Of "Internet Ready" Machines**

Virus's, most home user know that contracting a computer virus is a bad thing because of the popular press and the reports that have been in the news over the last few years. As most "internet ready" system come with Microsoft office or at the very least outlook express contracting a virus via e-mail is incredibly easy and once the home user system has a virus on it like a biological virus a computer virus will try to establish a hold over the host, then use the host to propagate to other systems.

Zombie systems, this is something that most home user would not understand as it does not generally effect that home user. With out correctly install security and antivirus the "internet ready" system can become one of hundreds of machines attacking a single target machine or network this is commonly referred to as DDOS.

Hacking or breaching a users system to allow them to gain access with out permission. This can lead to theft of id tokens and then fraud

## **5 why these attacks work**

All these attacks works because of the users lack of knowledge and the lack of security with in the systems. The lack of user knowledge is not something that can be tackled with ease due to time constraints and the user's will to learn and/or understand the technology behind the internet. However tackling the physical device that is allowing the crimes to take place can be done retails, consumers and government bodies can enable a Safety make such as the British safety flag for internet ready systems more details about this later (see 7)

## 6 What should a computer have to be internet ready?

For a computer to be internet ready it should be able to be plugged in and turned on and be safe and secure. To be able to achieve this a computer systems must have some basic thing such as firewall and antivirus software at least to be fully cased as internet ready the system should have all patches install including those that became available the day of the sale.

### 6.1 Antivirus

This piece of software can be free and commercial but should never be a set amount of days trail as this would mean that the computer system is only internet ready for the trail period

It is not only that it should be a fully licensed version but it should have the latest virus definitions and the latest patches for the virus scanner itself. This is because of the way virus's work. Most virus try to propagate by finding other systems that have not been patch and have the exploit still enabled, while a virus scanner would not stop the virus attacking the system, it would stop the virus from impacting the system by stopping the virus delivering its payload and stopping the infected files from propagating any further.

To further this the antivirus software should be configured to auto protect during run time and possibly do a registry scan at boot up, but most importantly it should be configured to auto update the virus definitions and virus scanner as soon as new up dates are available. This means if its virus resistant at the date of sale/delivery then it stay as up to date as possible.

As a virus attack can all but destroy a system with in five minutes of connecting to the internet and then launch attacks from that system. Most warranties that come with computer system do not include data recovery and hardware replacements due to virus infection damage. The question that should be asked about this is why this is so; if the system is internet ready is it not safe to say it should be able to defend its self against any virus that may attack the system with in a reasonable amount of confidence.

This does take in to account that someone most contract the virus and submit it to the anti-virus. However it is not normally the buyer of a "internet ready PC" that would be targeted as the1st target of a new virus

## 6.2 Firewall

This is a piece of software (it can also be hardware but in this case on off the shelf pc it is normally software) that should secure the system against external attacks and internal security breaches.

However poorly implemented firewalls and always-on connections can give the home user a false sense of security by making them think that there computers doors and windows are all locked. However most firewalls don't stop FTP and telnet by default and if the FTP and telnet port are open then the system can be found and is a visible target. Being visible aka not stealth means that ports send responses to unsolicited ping requests This is how port scanners work and with the open ports found other things can be done eventually leading to a compromised system.

So to summaries for a firewall to be classed as internet ready the retailer would need to know what services games the user will be running so the firewall can be correctly configured

## 6.3 THE Operating System

The Operating system is a major component to of the system and needs to be secure in order of the system to be secure. While no OS will ever be 100% secure that is the reason that patches and fix's come out for the Microsoft platform and that the open source OS such as some versions of Linux is played with by programmers to find security holes and close the. While on system can be 100% secure a poorly maintained OS can be the worse type of hole.

### 6.3.1 Windows

This is very dependent on the Operating System but as most "internet ready" system come with windows XP home edition with service pack 1 or in some case's 2 Let's look at the most optimistic view that the system was built around the beginning of September at this time the system was patched with the most up to date patch's for all of its software such as the OS office suite anti virus and firewall. The system is then packaged ready for shipping, it is placed in a warehouse till it an thousands like it are ready to be shipped to stores ready for there retail shelf life. an estimate from my own retail management past history for the retail shelf life is around four to eight weeks

this is on top of the warehouse shelf life which at best would be about a week.

So at a good time scale an "Internet Ready" system at time of purchase is on average eight weeks. Meaning that as soon as system is turned on and broad band is connected windows will ask the user if it should check for updates now or should remind them later if the user clicks now the updates are found, then the user is give some options as to how the update manager should work at best users should select automatically update and install all patches.

So while the windows patches are downloading the user is surfing the Web most lightly get a few pieces of spy ware if they are lucky if not they could find them self downloading a nice new glittering piece of free ware that didn't work when it was installed. Unknown that to user they have now downloaded last months system destroying virus which is now ready to fully install when the system is rebooted.

The windows update is finished and the popup box comes up with install complete please reboot to finalise, so the users clicks ok only for that pc to now be a zombie at best or at worse fail to boot up.

### **6.3.2 Linux**

Linux can be a cheaper alternative to the Microsoft OS, Linux can be made much more secure than windows however if you simply download Linux plus apache and all the add-ons it is very insecure and if this is the way that retailers ship the machines they are far from "internet ready" Linux setup and securing is not really a novice user task and as these "internet ready" systems are aimed at Linux is not that widely offered

How ever if it was to be offered it would most lightly not be internet ready due to the multitude of ways that Linux OS can be set up this coupled with the fact that Linux is see as the computer professional OS and hard to use wouldn't help make the system more "internet ready"

## **7 Possible solutions**

There is a clear need for a security standard to be established in order to be classed as internet ready such as firewalls and anti-virus, however this alone would not ensure a system to be internet ready. The system would need to fully patched before connecting to the internet with the un-patched

and venerable operating system. A quick solution would be a DVD/CD with all the patches updates as of the date of sale or delivery which ever is the later. However this would still not insure a fully internet ready system as this system may not be connected to the internet for some time and thus return to a venerable state.

A solution that will be fully detailed in another paper which will carry the technical specification at a later but the basic's details are as follows.

The system will have a hidden partition on the hard drive (or this could be firmware on to a mother board chip), on this partition will be stripped down version of a Linux installation that will connect to a secured line in order to download all the updates and patches it will then install them. This will all be done when the system boots if the system can not connect to the secured connection it disables all network connection and any other device and options that will enable internet access, the system will keep rechecking for the connection on each boot there after. If the system is able to connect it will of course enable internet access it will set all setting to maximum security setting as default enabling only web browser and email. If the user wish's to alter these setting with in the operating system they will be able to.

The final stage of what is need would be a small background program that runs along side the operating system that will monitor the systems run time as with always on internet connections becoming the normal is more than lightly that the system may stay turned on with out a reboot for weeks if not months, this program would ask the user periodically if they wish to retain there internet ready integrity if they are running as a privileged user or if the user is an unprivileged user it would till them that the system need to reboot in order to maintain the integrity and give them a few minutes to save any work and disable the internet connection or restart this would combat people that tend to click cancel to most security updates. The system would then reboot and boot in to the Linux install and do the automated updates.

With the system as detailed above in place along with the current antivirous software checking for updates while the operating system is running and windows updates set to automatically download and install all patches this is something that would be enabled via the linux partition. It would give a true "internet ready" system

As mentioned earlier in the paper this would allow a body such IFW the internet watch foundation to give out stamps or certificates of internet ready and thus giving the consumer something to look out for when buying

a computer for the internet.

## 7.1 What Could Be Done Right Now?

The first thing that can be done as a temporary measure is to stop calling them "internet ready" and change their name to internet enabled system. Another short term measure to help while the system and infrastructure is being developed, would be to use the DVD/CD method mentioned in section 7

This should do two things the first one being all the up to date patches and fix's for all the software installed on that system the system should not boot up till this disc is installed.

The second part of the disc should be aimed at informing the user of how to stay safe on the internet and raise the user's awareness.

The consumers that purchase system with the DVD/CD option could then be set and auto install version on the updated method when it is ready, that will install the partition and the secure connection Linux system and thus keep their system within the "internet ready" validation system.

## References

- [1] R Clarke. Technological aspects of internet crime prevention, February 1998.
- [2] R Clarke. Identified, anonymous and pseudonymous transactions, June 1999.
- [3] Crown Court. Computer misuse act 1990. [http://www.opsi.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm), 1990.
- [4] M Evans D E. Brown, L Gunderson. Crime mapping for computer crimes. Proceedings of the 2000 IEEE, June 2000.
- [5] W Boni DR GL Kovacich. *High Technology Crime Investigator's Handbook*. Butterworth Heinemann Elsevier, 10 edition, 2002.

- [6] B Etter. The forensic challenges of e-crime. In *Indo-Pacific Congress on Legal Medicine and Forensic Sciences*. Australasian Centre for Policing Research,, september 2001.
- [7] J Vandewalle J Claessens, B Preneel. Anonymity controlled electronic payment. Technical report, Katholieke University Leuven,, May 1999.
- [8] S Jansson L Rasmusson. Simulated social control for secure internet commerce. Proceedings 0-89791-944-0, Swedish Institute of Computer Science, Bos 1263, S-164 28 Kista, Sweden, 1996.
- [9] E Casey MG McGrath. Forensic psychiatry and the internet. *J Am Acad Psychiatry Law*, 30(1):81 94, 2002.
- [10] N Morris-Cotterill. Use and abuse of the internet in fraud and money laundering. *International Review of Law, Computers and Technology*, 13(2):211 228, August 1999.
- [11] E Quayle MTaylor. *Child Pornography: An Internet Crime*. Psychology Press (UK), 2003.
- [12] Home Office. *Code Of Practice*. Home Office.
- [13] R E. Worden R B. Parks. Community policing in action. resreach preview, Indiana University, State University of New York Albany, june 1998.
- [14] K Pease R Davis. Crime, technology and the future. *Security Journal*, 13(2):56 64, april 2000.
- [15] J MacGill S Openshaw, I Turton and J Davy. Putting the geographical analysis machine on the internet. Technical report, University of Leeds, Leeds LS2 9JT, 1998.
- [16] M S. Scott. Problem-oriented policing: Reflections on the first 20 years. Technical report, U.S. Department of Justice, Office of Community, Washington D.C, October 2000.
- [17] J R Vacca. *Computer Crime Scene Investigation*. Charles River Media, 2002.
- [18] D S Wall. *Crime and the internet*, volume 1. routledge, 2004.

[19] P Williams. Crime, illicit markets and money laundering. page 106 150.

[20] P Williams. Organized crime and cybercrime:, august 2001.