

Transferring crime fighting methods to the internet

Arron Martin Zeus Brown, Bsc,
University of Teeside
SSTUK

August 7, 2006

Contents

1	Introduction	2
2	Computer Crime	2
2.1	What is Crime?	2
2.2	What is Computer crime?	3
2.3	What is Internet Crime?	3
2.4	Summary	3
3	The problems with current methodologies	4
4	Reasoning behind the concept	5
5	Possible solution	5
6	Policing policies	8
6.1	Passive policing	8
6.2	Proactive policing	9
6.3	Reactive policing	10
7	Conclusion	10

List of Figures

1	figure i	7
2	figure ii	8

1 Introduction

The invention of the internet is now considered to be old, however it is the new ground where crime fighting must be taken to. The problem with trying to combat crime on the internet is that there is very little protocol in place, and crime fight tools tend to be aimed at those with scientific back grounds.

This paper looks at the growing crime rates on the "world wide internet" and the many other names it has been given. However maybe we should call it the old Wild West, as it is coming to the stage where the average user can be attacked, conned or even have there home broken into via web cams and microphones. In what we can call the "real world" the law enforcement agencies around the world have developed crime prevention and detection methods. It is these policing methods that have stopped the criminals running riot on the public streets and this paper looks at methods and there transposability on to the world wide internet. At the present time, the state of the internet leaves protection in the user's hands and in the hope that they will install antivirus and firewalls.

2 Computer Crime

To answer this question we must define what crime is, then what computer crime is, this should leave us with the internet as a definable region. It is the aim of the piece to clearly describe what internet crime is and how real world laws and surveillance techniques can be applied in the electronic world of the internet.

2.1 What is Crime?

This is a act of criminal activity that takes place in the real world and the criminal act must be committable without the use of a computer or electronic device, for instance the theft of a computer for an electronics company is classed as a crime even though it has involved computers. The computers

play no part in the crime being carried out, but it was one of the crime scenes.

2.2 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.

2.3 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.

2.4 Summary

The true grouping therefore must be listed as : None technology aided crime. Technology based crimes and its four categories.

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

3 The problems with current methodologies

The methodologies for capturing and seizing the hardware from a computer aided crime are in place even though in some places it is vague at best as to what the correct procedure is, for example the procedure for the removal of computer hardware states that the PC should be turned off via the plug at the rear of the PC, in some cases this can cause data to be damaged or destroyed. The best way for this procedure to be performed would be to have someone who is a computer forensic scientist attend each seizure and then decide the correct method of shut down.

These procedures say very little about what to do if the target of the seizure is a server nest with something like 10 or more server type systems or even in the modern house hold where there maybe 2, 3 or even more desktop system's networked together.

The guidelines say very little about the remote capture of data or the remote surveillance of a suspect or suspect system.

If we have a suspect there is very little evidence that we can gain to tie them to a machine without actually seeing them at a machine, if it is a shared machine this can be the main defence tool use by the defendant, so this is one major stalling block at the current time.

In the USA they have started to tackle these problems by laying out guidelines, the 9/11 attack was the main catalyst, they used the terrorist attack and the way they got there funding (via internet being one of many ways). In the guidelines [2] they layout what is classed as seizure material, wiretapping and other such guidelines.

The final problem lies with the end user, the average home user using ADSL may not even know when they have been compromised and embarrassment may stop them from reporting any crimes.

4 Reasoning behind the concept

The technologies to fight internet crime are available to the public but many people don't know how to use them correctly, this in general is also true for law enforcement agencies around the globe, with very few exceptions. Most police officers regardless of rank or age, are not up to date with current crime fighting tools.

The way forward is a clear one, the analogies and similarities must be shown between current real world situations that the average police officer may find themselves in and this is the concept of the migration of "real world" crime fighting methods to the internet.

This can range from the simple solution to explaining that a server is like a hotel where the address equals the URL, the hotel name is the IP address and the doors inside the hotel are the ports on that server and finally the guests in the rooms is the services running.

The police have looked at the internet as an area that needs special teams for now, while some parts of this maybe true it is also plausible that given the right guidelines and case studies it should be possible for all officers to understand.

5 Possible solution

One of the first things we need to do is something that the police forces through out the world do and that is categorise the areas we need to police and try to establish some sort of risk assessment. Some work in this area has been done by A Marshall, a formula for the victim's safety is one thing we can look at but we also need to look at the environment. This is the same as looking at a low income housing estate, where the crime rate is proven to be high over a time period it is given a higher risk assessment level, however you would not expect to have a bank robbery in this area, due to there being no banks on the house estate. It is this further consideration that the police use to deter crime as best that is possible. If we take this and relate it to the internet we can see some basic areas that needs to be policed

1. Chat rooms (this includes forums)
2. Chat programs (such as MSN IRC)
3. Emails (such as Spam, Phishing)

4. Online games (this is similar to chat rooms but with some added complications)
5. Warez internet (this includes the http and ftp servers along with the peer2peer file sharing methods)
6. Generic web surfing (this includes things like Google Whacking, searching for a holiday)

The environments all have the potential to produce what could be classed as a crime zone but this leaves us with the next area that needs to be categorised and that is the crime itself.

As we begin looking at the crimes and classifying them, the police force does this with real life crime such as a child stealing a penny sweet, being a misdemeanour to a high impact crime such as a murder. The internet holds a new set of values in that a human life can not be taken via the internet, as was looked at earlier the internet could be a means to an end, meaning that any murder would be an internet assisted crime and therefore the murder is not what this paper is looking at, however if we just look at the method, they used the internet to aid them, then this may be the crime we can target.

The main crimes on the internet at the moment can be categorised as;

1. Fraud (this includes many areas; bank attacks, Phishing)
2. Theft (this can include the theft of money, data or IP intellectual property)
3. Identity theft (this is gaining access to the tokens that are used to validate that someone is how they say they are)
4. Money laundering (this crime is that is done by organised gang's crime syndicates etc)
5. Grooming (this is the actions that an attacker will use on a victim to gain their confidence this is commonly found in paedophilia and child murder cases.)
6. Vandalism (the act of breaking into a web server and editing home pages of major companies however this trend seems to be on the down fall)

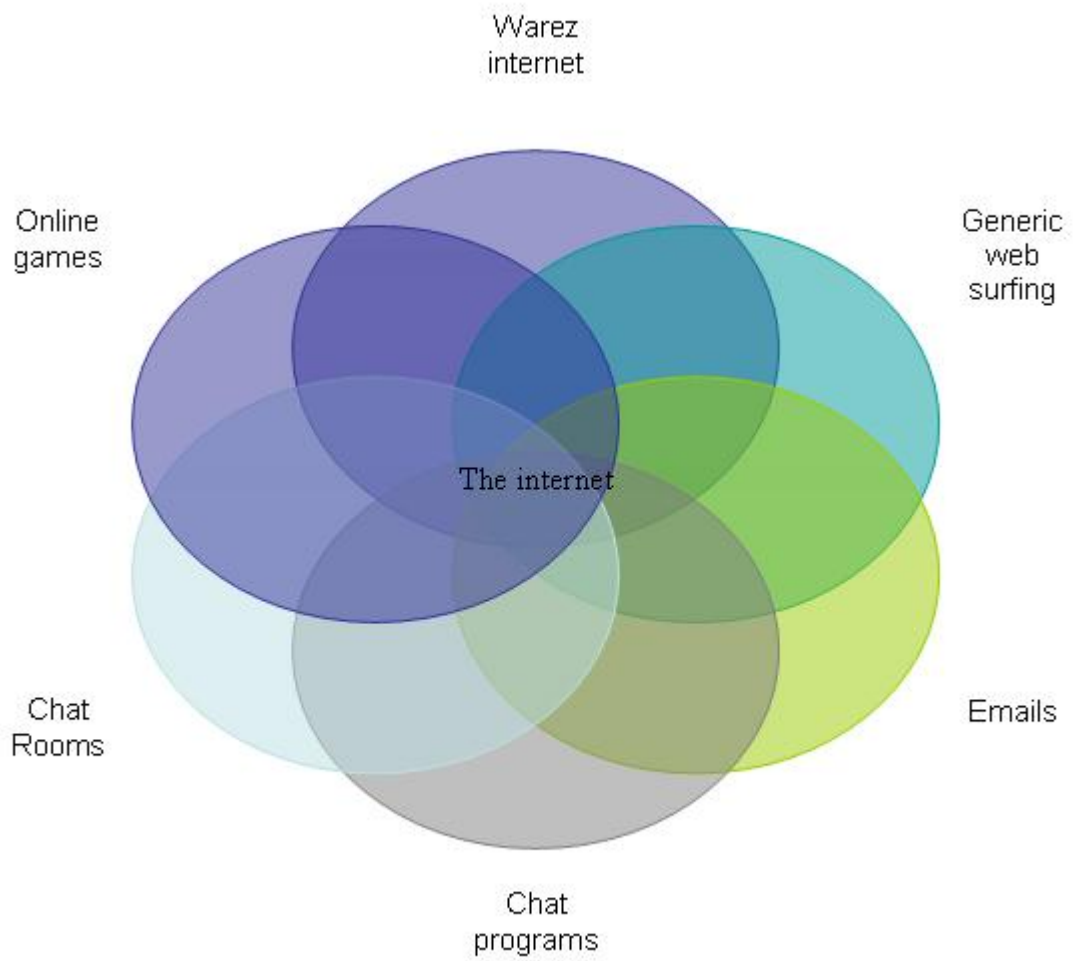


Figure 1: figure i

7. Terrorism (this crime can be but not always be carried out by activists)
8. Service attack (this crime cover things such as DDOS (distributed denial of service))

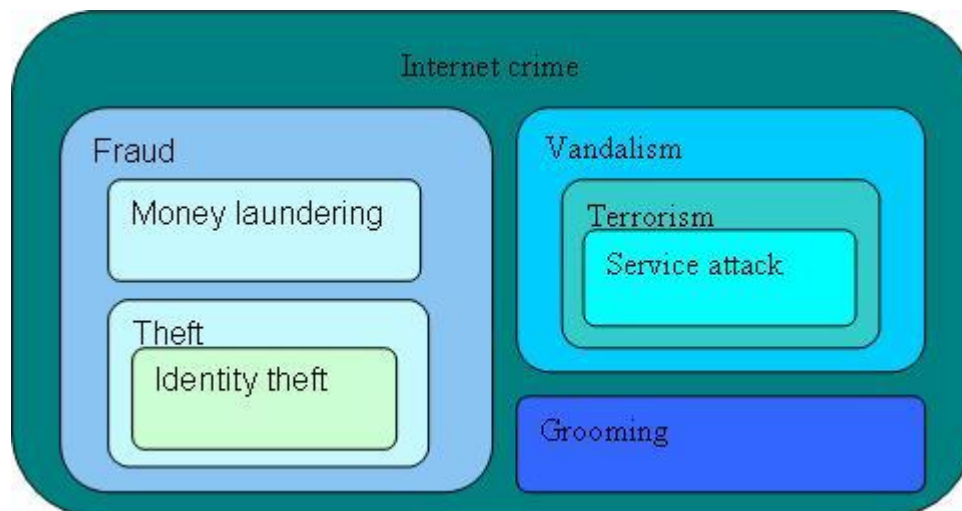


Figure 2: figure ii

The above is only a sample of internet crime there is always newly developing crimes and the model would need to be a constantly evolving one.

6 Policing policies

Policing can be divided into distinct types, there is passive policing proactive and reactive.

6.1 Passive policing

This is a policy that makes an area secure, in the real world this can be CCTV, good street lighting and the emergency telephone number. If we look at the internet we see that there are many dark corners for criminals to hide and no emergency phone number.

It has been proven that CCTV does cut crime levels so we need to look at having the same sort of concept on the internet.

A simple network of sensors that acts something like the distributed IDS (intrusion detection system). This system could passively monitor traffic patterns on the internet with out investigating any IP (internet protocol) address, therefore this policing method is not targeted and does not require an order for a surveillance to be carried out. As the content would not be investigated and the IP address not disclosed by the system, DP (Data Protection) could be withheld in accordance with the DP act.

Also monitoring and detection of crime on the internet by the use of commonly available resources on the internet, this could be looked at as the neighbourhood watch system that is in many housing areas the police interact with this system in the way that the people in the neighbourhood watch and report any activity that is out of place or suspicious to the police.

The final thing that needs to be put in place is the emergency phone number, while having a real phone line would prove technically expensive and difficult given all the differing laws languages and other real world policing barriers. There are many databases on the internet that collate information about areas that relate to computer crime, one example would be <http://www.spamhaus.org/> this database could be accessed to look at the possibilities of detecting Phishing attacks being done. However not all attacks are logged here and as the data is public some people may question its validity. A simple solution could be a central information repository where any internet crime is reported and all information relevant to that crime stored there. The law enforcement agency could then act upon it.

6.2 Proactive policing

This policy is about taking action before a crime is committed, a real world example of this is community policing, the officer on the beat. This type of policing uses visual police presence as a deterrent.

With the growth of chat rooms an automated monitor could be placed to identify key words patterns etc, again the automated Bot could be place to monitor traffic signatures with out examine to content.

The bobby on the beat methodology could then lead towards the warranted surveillance methodologies. In the real world policing there are many ways that this can be done, from undercover policing to remote surveillance such as wire tapping and video and audio recordings. Again these methodologies can be transposed onto the internet, the undercover police officer can be using some of the many forums, chat room and IRC (internet relay chat)

in order to gather intelligence and possible evidence, its is common for people known as "lamers" to try and take credit for hacking, cracking and other such attacks in order to try and earn kudos from within the cyber community, so this information gathered from these sources while not always 100% reliable is easily verifiable by simply asking how they performed the task, if they tell a tale that does not match what happened in the logs then they can be placed on a lower ranking for investigation.

The remote surveillance area of investigation is somewhat more difficult as some internet connected systems fall outside of the local policing authority and in some cases servers and ISP internet service providers almost start to aid and abet criminal activity by not keeping any logs of activity performed on that server.

If the IP address can be resolved correctly, in that I mean that if the IP has been spoofed it has be adjusted and resolved correctly, it is possible to obtain a wire tap similar to a wire tap for a phone, however it is possible to wiretap the internet connection but this will use a great deal of resources if the data is to be filed and stored. However it could be possible to have a system examine the data stream for patterns and record and useful information such as files that are being transferred either uploading or downloading. Other information that is good to collect would be packets that contain data that matches a predefined data set such as the control signals for a DDOS attack that is sent to each of the zombie machine.

6.3 Reactive policing

This is the main current method used on the internet in that the crime has happened and the action is a response to that crime, however this methodology is not good enough for what is the world biggest market place, meeting place and every thing else it can be. So we must look at the other two.

7 Conclusion

While the internet grows in age the policing methods currently used on it are some what trailing behind the technology that is being used by the criminals that are using this technology. The technologies and data is available to enable better policing methodologies. However at the present time there are no tools for the average police officer with out a computer forensics science

back ground to enable him to investigate an internet crime, this means that these crimes often go unsolved due to lack of man power that is able to be invested. However if the tools were developed with the user in mind and made simple and clear to understand, the average PC (Police Constable) could follow his lines of enquiry then hand over the case and report at the stage where the data needs to be examined by a human. This would mean that the specialist teams would be able to examine the reports and data collected without the need to collect the data. This would mean that they could work through the data much quicker, this is just like how the forensic labs function, for example they receive two DNA samples and ask to see if they match. They are not asked to investigate the crime, they are only to examine the evidence.

References

- Clarke, R.: 1998, Technological aspects of internet crime prevention.
- Clarke, R.: 1999, Identified, anonymous and pseudonymous transactions.
- D E. Brown, L Gunderson, M. E.: 2000, Crime mapping for computer crimes, Proceedings of the 2000 IEEE.
- DR GL Kovacich, W. B.: 2002, *High Technology Crime Investigator's Handbook*, 10 edn, Butterworth Heinemann Elsevier.
- Etter, B.: 2001, The forensic challenges of e-crime, *Indo-Pacific Congress on Legal Medicine and Forensic Sciences*, Australasian Centre for Policing Research,.
- J Claessens, B Preneel, J. V.: 1999, Anonymity controlled electronic payment, *Technical report*, Katholieke University Leuven,.
- L Rasmusson, S. J.: 1996, Simulated social control for secure internet commerce, *Proceedings 0-89791-944-0*, Swedish Institute of Computer Science, Bos 1263, S-164 28 Kista, Sweden.
- M Gill, A. S.: 2005, Assessing the impact of cctv, *Home Office Research Study 292*, Home Office Research, Development and Statistics Directorate.
- MG McGrath, E. C.: 2002, Forensic psychiatry and the internet, *J Am Acad Psychiatry Law* **30**(1), 81 94.
- Morris-Cotterill, N.: 1999, Use and abuse of the internet in fraud and money laundering, *International Review of Law, Computers and Technology* **13**(2), 211 228.
- MTaylor, E. Q.: 2003, *Child Pornography: An Internet Crime*, Psychology Press (UK).
- Office, H.: n.d., *Code Of Practice*, Home Office.
- R B. Parks, R. E. W.: 1998, Community policing in action, *research preview*, Indiana University, State University of New York Albany.
- R Davis, K. P.: 2000, Crime, technology and the future, *Security Journal* **13**(2), 56 64.

- S Openshaw, I Turton, J. M. and Davy, J.: 1998, Putting the geographical analysis machine on the internet, *Technical report*, University of Leeds, Leeds LS2 9JT.
- Scott, M. S.: 2000, Problem-oriented policing: Reflections on the first 20 years, *Technical report*, U.S. Department of Justice, Office of Community, Washington D.C.
- Vacca, J. R.: 2002, *Computer Crime Scene Investigation*, Charles River Media.
- Wall, D. S.: 2004, *Crime and the internet*, Vol. 1, routledge.
- Williams, P.: 2001, Organized crime and cybercrime:.
- Williams, P.: n.d., Crime, illicit markets and money laundering, p. 106 150.