available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The growing phenomenon of crime and the internet: A cybercrime execution and analysis model

Paul Hunton

Cleveland Police, Middlesbrough, UK

Keywords:
Cybercrime
e-Crime
Internet crime
Hi-tech crime
Police
Criminal investigation

ABSTRACT

The aim of this paper is to demonstrate the opportunities to law enforcement when investigating the cyber criminal by defining an emerging cybercrime execution model. The model is intended to enable the transference of conventional policing models into an often abstract and technical environment. The background context is first given, and then a description of the distinct components and characteristics of the cybercrime execution and analysis model is presented. The model is aimed at structuring and focusing the evaluation and decision making process when investigating and analysing highly technical and complex cybercrimes. The objective of the model is to provide a consistent means of examining each piece of a potential cybercrime puzzle in turn. This paper concludes by identifying the advantages of such a model to facilitate new and innovative investigation practices and procedures by breaking down the many technical challenges faced when investigating crime and the use of networked technology such as the Internet.

1. Introduction

The aim of this paper is to demonstrate the opportunities to law enforcement when investigating the cyber criminal by defining a cybercrime execution and analysis model, which will better enable the transference of conventional policing models into an often abstract and technical environment.

The background context is first given, and then the distinct components and characteristics of the cybercrime investigation and analysis model are presented. The aim of the model is to simplify the complexity of cybercrime investigation and to provide investigators and analysts at all levels with specific points of reference to conceptualise the common components and abstract activities where reliable evidence, criminal intelligence and analysis data can be found.

In conclusion the model presented in this paper is aimed at assisting a cybercrime investigator to plan complex technical investigations, formally consider the technology and techniques used and consistently examine each piece of a potential cybercrime puzzle in turn.

The future use and development of the model is aimed at establishing a practical investigative tool that can be used to facilitate new and innovative practices, policies and procedures by breaking down the many technical challenges faced when investigating crime and the use of networked technology such as the Internet.

2. Background

With the rapid adoption and continued development of the Internet over the past decade, it has become commonplace for individuals and organisations alike to have so-called 'virtual' or 'cyber' existences that are intrinsically entwined with physical real world presence.

With the continued advance of technology, the Internet delivers much more than the flat or simple information once found. The Internet enables real-time dynamic interaction, facilitating global opportunities such as rapid communication, socialising, information and data sharing, banking, the

0267-3649/$ – see front matter © 2009 Dr Paul Hunton. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2009.09.005

sale and purchase of goods, and a vast array of business activities and information services. The growing economic implication of the Internet is highlighted when considering that during 2007 online UK shopping transactions reached £34 billion (Garlik, 2008) and figures show that even in an economic down turn unique visitors to major retails sites were up by over 35% in quarter 4 of 2008 compared to 2007 (Nielsen Online, 2009). It is further estimated that by 2012, 20% of all new UK commerce will be online (Carter, 2009).

From a UK Government perspective, the success of digital networks is seen as essential. Gordon Brown, the Prime Minister when introducing the report Digital Britain stated that ''Only a Digital Britain can unlock the imagination and creativity that will secure for us and our children the highly skilled jobs of the future. Only a Digital Britain will secure the wonders of an information revolution that could transform every part of our lives. Only a Digital Britain will enable us to demonstrate the vision and dynamism that we have to shape the future.''

The magnitude of our cyber existence becomes more apparent when considering that an estimated three billion e-mails are sent every day in the UK alone (BBC News, 2009b), and the social networking sites MySpace and Facebook have a joint user base of 270 million and received 2.8 billion visitors between March 2007 and 2008 (Garlik, 2008). It is now estimated that 65% of all UK households have Internet access and of those who do not a further 13% have Internet access elsewhere, for example work or school (Office for National Statistics, 2008; Eurostat, 2008).

Broadband now accounts for 94% of all UK Internet connectivity (Office for National Statistics, 2008). In the recent BERR (2008) Information Security Breach Survey it was identified that 97% of the UK businesses surveyed had broadband Internet access and 84% of these businesses were also heavily dependant on their IT systems for conducting business. These figures account for an estimated 40 million UK users with the majority of young people aged 9–19 accessing the internet every day (Garlik, 2008; Livingstone and Bober, 2004).

The global adoption of the Internet is equally reflected throughout Europe with an average of 60% of households having Internet access (Eurostat, 2008). This increases to over 70% in the USA (IWS, 2009). Add to this the large range of mobile and handheld devices that can provide direct access to the Internet and share resources on the move then the scale of the Internet phenomenon is currently estimated at 1.4 billion users worldwide (IWS, 2009).

However, as is common with general advances in technology, as the benefits become apparent then so do the new opportunities for criminal and undesirable behaviours (Bryant et al., 2008). With the ease of access to such large scale global cyber freedoms then the undesirable side of the Internet also presents unscrupulous individuals with the opportunity to exploit and prey on the opportunities on offer in a 'cyber' world. The term now commonly used to describe the unacceptable side of the Internet is 'Cybercrime'.

2.1. *So what is cybercrime?*

The concept of 'digital' or 'hi-tech' crime where technology is used to support or directly facilitate criminal activity is nothing new (Wall, 2007; Bryant et al., 2008). Likewise, 'cyber' is a term commonly used to describe the perceived virtual environment associated with the Internet. In recent years the term 'cybercrime' has become commonly adopted by the media, academia, law enforcement and Governments alike to discuss and debate the issues of technology-related crime and in particular the Internet.

It is becoming increasingly accepted that the term cybercrime is used as a convenient label to describe crime and other illicit activities that involve the use of networked technology (Bryant et al., 2008; Cross, 2008; Moulton, 2008; Wall, 2007; Yar, 2006). However, an exact definition of cybercrime is still unclear (Garlik, 2008) and at present there is no formal scientific or legally agreed meaning (Wall, 2007; Bryant et al., 2008). This is likely to continue as cybercrime is still considered in its infancy and different types of cybercrimes are likely to emerge as technology continues to advance.

From the perspective of law enforcement, it must also be acknowledged that not all so-called cybercrimes are necessarily crimes under the criminal law (Wall, 2007; Garlik, 2008). Cybercrime as a concept is much broader than just crime alone as it also covers the wider issues of unacceptable or undesirable behaviour (Yar, 2006). However, with no specific reference point in UK law (Wall, 2007; House of Lords, 2008) or agreed classification of technology-related crime (House of Lords, 2008), the ability to distinguish or quantify the true scale and criminal nature of cybercrime remains extremely difficult.

Therefore, for the purpose of this discussion cybercrime is a general term of convenience and is considered a subset of 'digital' or 'hi-tech' crime and as a generalisation for criminal and undesirable or harmful behaviour that is assisted or enabled by networked technology.

2.2. *The growing phenomenon of cybercrime*

Grabosky et al. (2001) suggest that the fundamental principle of criminology is that crime follows opportunity. As the Internet and underlying networked technology has continued to develop and grow then so has the opportunity for illicit behaviour. Utilising digital networks such as the Internet provides cyber criminals with a simplified, cost effective and repeatable means to conduct rapid large scale attacks against a global cyber community (Bryant et al., 2008). Using methods such as email and websites eliminates the need for face-to-face communication and provides the cyber criminal with a level of anonymity that reduces the perception of risk and also increases the appearance of legitimacy to a potential victim (Fletcher, 2007).

With a majority of young people now accessing the Internet every day combining with the growth of online communication channels such as social networking sites, the opportunity for cybercrime can be seen to extend the broader reaches of our global society. The young and vulnerable are also targeted by cyber criminals through activities such as online grooming, cyber-bullying, pornography and paedophilia, along with being exposed to additional peer pressure and other unacceptable behaviours (Byron, 2008). Common examples of cyber related crimes can be demonstrated by such offences as fraud, identity theft and theft of Intellectual