Research in Progress Short Paper: The Adoption of Criminal Profiling for Computer Crime

Joerg Preuss
Bundeskriminalamt, Germany &
University of Plymouth, United Kingdom

Steven M. Furnell
Network Research Group, University of Plymouth, United Kingdom

Susan J. Lea
Faculty of Health and Social Work, University of Plymouth, United Kingdom

About the Authors

Joerg Preuss holds a law degree from the University of Frankfurt, Germany and a degree in Informatics from the University of Applied Science Darmstadt, Germany. He works as a researcher at the Institute of Criminology from Bundeskriminalamt – the German Federal Police Office. He is also working on his Ph.D. at the Network Research Group of the University of Plymouth, England. His research interests include criminology and criminology related to computer crime, secure communication, and computer networks.

Mailing Address: Joerg Preuss, Network Research Group, School of Computing, Communications & Electronics, University of Plymouth, Drake Circus, Plymouth, PL4 8AA, United Kingdom; Tel. +44 1752 233521; Fax: +44 1752 233520; Email: joerg@preuss.info

Steven Furnell is the head of the Network Research Group at the University of Plymouth. He is currently leading research in relation to user authentication and intrusion detection technologies, with related research into the analysis of computer crime and information warfare. Dr Furnell is the author of over 120 published works, including the book 'Cybercrime: Vandalizing the Information Society', published by Addison Wesley.

Descriptors

blackhats; computer crime; cyber crime; criminal; profiling; behavioural; psychological; law enforcement; inductive reasoning; deductive reasoning; system analysis; network analysis

Reference to, or **Citation** of this paper should be made as follows:
Preuss, J., Furnell, S. M. & Lea, S. J. (2004). Research in Progress Paper: The Adoption of Criminal Profiling for Computer Crime. In U.E. Gattiker (Ed.), EICAR 2004 Conference CD-rom: Best Paper Proceedings (ISBN: 87-987271-6-8) 16 pages. Copenhagen: EICAR e.V.

Research in Progress Short Paper: The Adoption of Criminal Profiling for Computer Crime

Abstract

This paper discusses ongoing research in relation to the adoption of criminal profiling for computer crimes. It begins by introducing the concepts of psychological, behavioural or criminal profiling used in traditional crime, discussing methods such as inductive reasoning or deductive reasoning, and then proceeds to outline computer forensic methods, which may be used to examine computer systems after an incident. It also discusses the possibilities and problems analysing network activities. The paper suggests how the methods of criminal profiling can be adopted for computer crime incidents, as an assistance of the investigations of law enforcement agencies against hackers, and other criminals who focus upon the computer to commit their crimes. To this end, the discussion presents a top-level mapping of behavioural evidence analysis within a computing context.

ISBN: 87-987271-6-8

Structure Of The Paper

Statistics from recent years have illustrated a dramatic rise in the incidence of cybercrimes, such as hacking, malware, and system abuse. For example, figures from Bundeskriminalamt (BKA) in 2001 identified 79,283 related incidents in Germany (Bundeskriminalamt, 2001), compared to only 45,359 in 1999 (Bundeskriminalamt, 1999). Similarly, CERT (2004) shows that there were over 80,000 incidents in 2002, an increase of about 30,000 compared to the previous year. For the year 2003, CERT reported 137,529 incidents showing that problems are occurring in spite of advances in network security technologies, and suggesting that a technological approach alone is not a sufficient basis for tackling the problem. To more effectively combat cybercrimes it is necessary to understand the reasons and motivations for incidents, and the methods by which they are perpetrated, and then use this as a means of informing investigation and detection activities.

This paper will explain the concept of criminal profiling, which is used to provide a picture of an unknown offender, by analysing his or her crime perpetration. The paper will also consider ongoing research relating to how these methods can be used for computer-based crime. The discussion begins by presenting a background to the profiling concept, before proceeding to review the common approaches used within traditional criminal investigations. The desirability of profiling computer criminals is then considered, leading to an overview of the accompanying technical methods that could be used to assist the evidence gathering process. The results section shows how these methods can be mapped into a behavioural evidence analysis approach, in order to provide a potential top-level profiling method for computer crimes.

When the paper refers at the male perpetrator, it is always meant the male and female criminal.

Literature Review

Criminal Profiling is a method to understand the mind of an unknown perpetrator or to gain an insight into how the perpetrator behaves if a specific situation occurs (Turvey 2003, p. xxi). There are different or modern approaches of e.g. Bundeskriminalamt (German Federal Police Office), that considers all the facts of a crime and focus on crime reconstruction, instead of focussing the development of an offender profile. (Baurmann 2003, p. 8)(Dern & Witt 2002, pp. 115-116)

The origins of profiling can be traced back many centuries. For example, Turvey (2003, p.2) cites an occurrence around 1486, where a guide was published about identifying witches. Turvey's quotation of the authors of that guide illustrates the problematic nature of unproven assumptions, made just from impressions. If there are few facts that serve as a basis, then such a profile has little value. Even today, many profiles could not truly be described as scientific work, and indeed there is much discussion about whether profiling is a science or an art

ISBN: 87-987271-6-8

(Canter, 1998) (Hoffmann & Musolff, 2000 p. 24) (Holmes, Holmes, 2002 pp. 13-15) (Turvey, 2003 pp. 42-44).

Modern criminal profiling is based upon several other disciplines: Criminology, dealing with the study of criminal behaviour itself; Psychology and psychiatry, dealing with the scientific study of human behaviour and mental illness; and forensic science, dealing with the physical evidence. Although there is no doubt about the sciences that build the basis, there is a wide range of methodologies within which they are combined. Conclusions are often based on statistical arguments, but sometimes also upon examining a specific criminal behaviour. One inference of the criminologists is the modus operandi (MO). The MO describes what the perpetrator did, at which time, how he reached his result, the tactics and methods, and the characteristics of his or her doing. In the early days of criminology it was assumed that a perpetrator could not vary his methods and tactics, and had no autonomy of decision about his/her MO. Today there exist doubts about this, and it is considered that a perpetrator is able to learn and to improve. (Turvey, 2003 p. 7, 65) (Douglas 1992, p. 260)

Profiling methods in general

Several profiling methods have been developed, and examples exist from the FBI (Federal Bureau of Investigation), RCMP (Royal Canadian Mounted Police), BKA (Bundeskriminalamt), and from several scientists and criminal profilers, such as Turvey, Britton, Canter and others.

As mentioned above, the research activity for profiling methods is based on the idea of the MO and the offender's signature. For a better understanding, it is necessary to explain the two basic differences to provide a statement about an offender of a specific crime.

Inductive criminal profiling. Inductive criminal profiling involves deriving rules from a set of specific cases or observations to form a generalisation – these generalisations are called premises (Turvey, 2003 p. 23)(Holmes & Holmes, 2002 p. 5). To build a profile in this way, observations of many crimes have to be analysed, to filter out clusters of signs and symptoms. The result then describes an average offender (of a specific crime) (Turvey, 2003 p. 26). Inductive profiling is not always based upon statistical methods, and in many cases the professional experience of a criminal investigator has to be the basis (Brock, 1999) (Hoffmann & Musolff, 2000 pp. 23-24) (Turvey, 2003 p. 22). A common opinion in the literature rates the professional experience higher than the statistical methods (Petherick, 1999).

Deductive criminal profiling. Deductive profiling differs significantly from the inductive reasoning. Rather than analysing a large amount of data from different cases, a profiler has to analyse a specific crime scene and the physical evidence that is discovered (Holmes & Holmes, 2002 p. 2)(Turvey, 2003 p. 35).

ISBN: 87-987271-6-8

As deductive criminal profiling deals with only one offence of a specific crime, the issue of professional experience becomes much more important (Hammond 1999). Results from an inductive criminal profile also support the process of reasoning during development of a profile in a deductive way (Turvey, 2003 pp. 36 - 37). Three methods of deductive criminal profiling are operational case analysis, crime scene analysis and behavioural evidence analysis, all of which are summarised in the paragraphs that follow.

Operational case analysis. The operational case analysis is a method developed by the BKA. (Baurmann 2003) The important point of the German approach is, that there is no focus to develop a profile. The aim of the OCA is to reconstruct and analyse the case.

- **Collection of information.** During this stage any kind of information has to be gathered, like autopsy reports, photographs, videos, maps, traces, facts and more. Those information have to be objective data, evidence given from witnesses has to be ignored at this point.
- **Decision-making process.** This step is used to provide information about the risk to the victim, the risk to offender, a case classification and the first impression about the primary motive.
- **Reconstruction.** A detailed analysis of the sequence of the offence has to be provided as well as a conduct classification.
- **Case characteristics.** This step reveals a conclusive classification of the motive, the victim selection and selection of the crime scene. The case characteristics also provide information about the aspects control, escalation, progression, staging, undoing and the dynamics at the crime scene.
- **Offender profile.** This stage is used to build an offender profile, regarding the offender's psychological and physical characteristics, education, present circumstances, previous convictions, home and anchor points and the offender's conduct before and after the offence.

Crime scene analysis. As the name suggest, this method is used to draw an impression of the crime's perpetration. This method was developed by the Behavioural Science Unit (BSU) of the FBI and is based upon six steps (Petherick, 1999):

- **Profiling input.** Any relevant information of the specific case has to be collected. Relevant information may include photographs of the crime scene, a background check of the victim, autopsy protocols, and any information that can be gathered about the time before, during and after the crime.
- **Decision process models.** Gathered information has to be arranged in a coherent and logical order. These developed patterns can highlight relations to
- one or more other crimes, which follow those patterns. This can establish the assumption of the perpetrator as a serial offender.

ISBN: 87-987271-6-8

- **Crime assessment.** The next stage is used to understand the role of the victim as well as the role of the offender, by reconstructing the sequence of events and the specific behaviour of victim and perpetrator.
- **The criminal profile.** This process deals with providing knowledge about physical and behavioural characteristics of the perpetrator. This knowledge may be used for tactical decisions.
- **The investigation.** The profile now has to be distributed to the investigating and requesting law enforcement agencies and the police officers. The profile has to be reassessed if no suspects are identified, or if new evidence is gathered.
- **The apprehension.** During this process the profile has to be cross checked against the characteristics of the offender who has been apprehended.

Behavioural evidence analysis. The Behavioural Evidence Analysis (BEA) is another method developed by Turvey and is an implementation of deductive reasoning (Turvey, 2003 p. 35). The BEA process falls into several parts (Turvey, 2003 p. 41):

- **The equivocal forensic analysis.** A full forensic analysis has to be performed. This includes physical evidence, witness statements and/or the corroboration of the two. This has to be done to establish the victim and the offender's behaviour by reliable sources.
- **Victimology.** Victimology is an important step of BEA, and is a form of risk assessment. The knowledge of the victim's characteristics can give the investigators a hint about the offender's motive, MO and the determination of offender fantasy behaviour. As such, it is necessary to spend a lot of time profiling the victims.
- **Crime scene characteristics.** The next step is to analyse the crime scene characteristics. For example, Turvey (2003, pp. 41 – 42) lists the method of approach, method of attack, method of control, location type, nature and sequence of sexual acts, materials used, any verbal activity and precautionary acts. These characteristics are determined from the forensic evidence and the victimology, and can help the profiler to discriminate between modus operandi (MO) and the offender's signature behaviour. Turvey (2003, pp. 65, 66) describes the differences between these as follows:
  "The MO is a summary of habits, techniques and peculiarities of behaviour of an offender that varies with the growing experience of the offender. Whereas the signature behaviour means that the behaviour of the offender must be so unusual and distinctive as to be like a signature".

  Douglas (1992, pp. 260 - 261) describes it, with simple words. The specific MO is used by the offender, because it works. The offender is able to commit the specific crime. The signature behaviour (Douglas calls it signature aspect) is a unique behaviour, that is developed by the

ISBN: 87-987271-6-8

offender's fantasies and which are need to be expressed by this special behaviour.

Having considered the basis of these approaches, it is also relevant to examine the applicability of profiling in the context of computer crime.

Computer Crime Profiling

Turvey (2003, p. 547) writes that criminal profiling has much to offer when a network such as the Internet is involved. The process of developing a profile using the classical criminalistic methods is infeasible for cybercrime, and it has to be used in a different way. To this end, the inductive and the deductive reasoning methods can be re-considered in the context of cybercrime:

- **Deductive reasoning.** For deductive profiling or behavioural evidence analysis the equivocal forensic analysis has to be performed, and the victim has to be profiled (Victimology). At least the crime scene characteristics have to be worked out. The use of the Internet generates footprints of the offender (Casey, Larson & Morrow Lang, 2003 p. 201). These can help to establish the behavioural aspects of the victim and the offender. This procedure is very similar to the equivocal forensic analysis for non cybercrime cases, but the analysis has to be performed in a different way (for some aspects). The primary investigation activity has to be reviewing audit trails, instead of interviewing potential witnesses, neighbours.
- **Inductive reasoning.** Inductive reasoning could also be used for cybercrime profiling. The problems will be the same as for the common psychological profile, in terms of the necessity to gain a large amount of data, describing the offender's demographic characteristics as well as the behavioural aspects. As mentioned above, inductive reasoning can reveal clues to an investigator that provide input for the process of deductive reasoning.

Several papers and books exist, that deal with hacker or computer criminal taxonomy. Sometimes it is talked about hacker profiles (Turvey, 2003)(Icove, Seger & VonStorch, 1995)(Halleck, 2003)(Howard & Longstaff, 1998). However, much of the work to date is actually more related to categorisation of the attacks themselves, and little prior work has been conducted in relation to the profiling of cybercriminals from a psychological perspective. Much of the existing material appears to be based upon anecdotal stereotypes rather then objective evidence.

It is important to understand what types of offender are described by those taxonomies. Both Turvey (2003, pp. 549 – 552) and Furnell (2002, p. 3) distinguish between criminals that use the computer merely as a tool to commit their crimes, and those where the computer is the target of their action. Furnell (2002, p. 3) calls it computer-assisted crime and computer-focused crime. Several works also try to describe the hackers' characteristics, with discussions

ISBN: 87-987271-6-8

about the skill and the motivations of the perpetrators. This results in hackers' classifications such as "Script Kiddies", "Lamers", "Warez Dudez", "Uber-Hackers", "Black-Hats", "White-Hats", and others. The term 'Script Kiddie' for example, is used to refer to immature hackers who are not able to develop their own exploits, and therefore rely upon using prewritten scripts and tools, downloaded from the Internet, to support their activities. Meanwhile, Warez Dudez' do not necessarily break into computer systems or try to distribute malicious software. Their motivation is to obtain and distribute free software - not in the meaning of open source, but any software as games, application software, tools or others (Schwartau, 2000 p. 44). However, while such descriptions provide a useful means of distinguishing the motives of cybercriminals at a general level, a genuine criminal profile has to be developed in a specific way, supported by statistical methods and/or common criminalistic methods, like equivocal forensic analysis, victimology and the analysis of the crime scene characteristics. The existing profiling efforts could be identified as a method of profiling using inductive reasoning. (Turvey, 2003 p. 551). They show off fewer characteristics that help to describe an offender in a way it is needed in law enforcement investigations. The way a "Warez Dude" is characterised can hardly help to draw a detailed picture of the perpetrator. It can probably help the investigators to understand the motivation, but a profile as described above cannot tell anything about the behavioural aspect such as what a perpetrator does to hide his footprints, or the tools he uses communication. In short, the existing taxonomy does not show off the MO or signature behaviour, that is one of the very interesting and important aspects of profiling. A more detailed description of the perpetrator could be provided by using the way of deductive reasoning, as it was shown before and described by the term Behaviour Evidence Analysis (Turvey, 2003 p. 35). Howard & Longstaff (1998, pp. 15 – 17) use the term "taxonomy" in a way that is very near to the forensic research that has to be done for providing a criminal profile.

Methods

As expressed above, there is a discrepancy in the understanding of profiling as an art or a science. The discussion shows that there are probably some aspects of profiling that could be supported by the scientific method. However, there are also cases in which professional experience, probably supported by inductive reasoning, seems often to be more attractive, due to the speed this method shows results (Turvey, 2003 p. 28). Deductive reasoning is a slower way to establish a profile, but it allows more detailed statements about the probable perpetrator. For the future research in this area the inductive reasoning could only be applied if there is a chance to gather the important data in such an amount, which allows the gathering of meaningful results from that sample. The data needs to be a combination of demographic and technical attributes, and there needs to be an appropriate number of suitably similar cases from which to base a sample. A promising way to create network attacker profiles is deductive reasoning, using Behavioural Evidence Analysis. In order to have some data to

ISBN: 87-987271-6-8

work from, this kind of reasoning has to be applied to information collected from computer forensics.

Computer Forensics

Computer forensic analysis has become a recognised means of providing evidence in computer crime cases (Noblett, Pollitt & Presley, 2000). There are several Computer Emergency Response Teams (CERT) (e.g. http://www.cert.org), and Interpol Working Parties on Information Technology Crime (http://www.interpol.com), law enforcement research groups, and civilian researcher and research groups who give rulebooks to forensic investigators.

For deductive reasoning the equivocal forensic analysis has to be performed. This is what Casey (2002) calls crime reconstruction. Casey (2002, p. 8) distinguishes between relational, functional or temporal clues, that could be gained. Relational clues describe interactions between objects, e.g. the use of a file and a tool to manipulate the file content. Functional clues describe the way something works and/or how it was used. The temporal clues describe the timeline for evidence and events.

System analysis. In this context, system analysis describes the forensic analysis of the file systems. This includes the detection of any deletion or modification of files and the file content, as well as the examination of log file entries.

File systems have to be duplicated, without any modification, before they are examined. Having duplicated the file system, the copy has to be examined. Several tools, such as “Sleuthkit” (http://www.sleuthkit.org) or “Encase” (http://www.encase.com), can be identified that can assist investigators in examining file systems.

A good way to reduce the job of the investigator (which is often necessary due to the large size of modern hard disks) is to find duplicate and already known material before starting the examination of the file system. Therefore it is possible to use the MD5 hash algorithm. The use of MD5 can help to identify those files that are not relevant, like system libraries or system commands. To do this, law enforcement agencies and computer forensic companies use so called hash databases (e.g. http://www.nsrl.nist.gov), that are filled with MD5 hash values of known files, that are irrelevant. The remaining files have to be analysed. Which files have to be analysed, depends on the crime that has been committed. In case of a hacking incident, it would at least be necessary to examine log files and configuration files.

Log files can show, what happened at which time. They also may reveal the application that was responsible for that event. Syslogd, for example, a logging daemon, an application that is typically available on Unix like operating systems, logs many different system messages. It is possible to notice that someone

ISBN: 87-987271-6-8

remotely logged into the system by reading system messages logged by syslogd. An attempt to login via SSH (Secure Shell, http://www.openssh.org) would be logged, if the system is configured that way. The log file entry would show when that event occurred and it also shows from which system (IP address) the login was initiated and which username was used to login. This behaviour is also to notice, if the username is a known one and the correct password was entered.

Various applications and servers, especially daemons, offer a logging facility. For example, the Apache (http://www.apache.org) web server uses log files, which reveal connections from systems that request web sites. It also has a file that holds logging entries for requests that produced an error.

Several Unix shells have history files. Those history files store any command the user typed. If a command or a path name or file name was misspelled, this is also stored in the history file of the shell. So reviewing history files can help to find modified files as well.

Log files are not the only interesting files that need to be examined. Configuration files, such as '/etc/passwd' that handles user entries on several Unix like systems, can show if someone created a new user entry, to login to the system. A modification of '/etc/shadow', such as a modified password hash for a regular user, could also reveal that a perpetrator has already compromised a system. The entries for group membership of system users could be modified in that way, that a user with standard permissions has superuser rights after that modification.

Beyond this, any other file could also be of interest. Documents that have an interesting content could be related somehow to the crime, prompting questions such as whether those files are still in the same location, whether they have been modified, and whether indeed they still exist. Forensic toolkits, such as those mentioned before, can be used to find answers for these questions.

Network analysis. Whereas system analysis is done by an examination of existing and accessible material, network analysis requires a specific environment. If there is nothing that logs incoming and outgoing network traffic, there is nearly no way to analyse anything network-specific after the crime was committed. However, if the network traffic is monitored, some aspects of the network traffic could be analysed.

If a network attack is detected and the attack lasts longer than just a few minutes, it can be possible to prepare some network related systems, like routers or gateways, to log the network traffic. It is also possible to monitor the state of a connection, with system tools like 'netstat'. 'Netstat' is a network status tool that prints out a table with connection entries. Activities initiated by Trojan tools like 'Back Orifice' or 'SubSeven' could be detected by reviewing this output.

ISBN: 87-987271-6-8

The network protocol itself can also offer clues. Although, it is possible for a clever criminal, or a cleverly coded tool, to manipulate several bytes (e.g. IP address) of the network packet, even this can be one piece in the puzzle.

Whether the whole traffic is logged or not, remote intrusion activities can often be detected by system analysis, as described above. A very interesting result of a network analysis could be the revealed tactics of the perpetrator.

Results

Criminal profiling is used to optimise investigation, to reduce the amount of suspects, to set up a risk analysis or, in the best case, to catch the offender (Musolff, 2002 p. 4) (Turvey, 2003 p. 1, 46, 47). For computer crime, the authors propose that profiling could be used in the same way, respectively to achieve the same objectives. An example of the associated process is illustrated in Figure 1, it describes an example offender and an example victim and some of there possible characteristics. First of all the equivocal analysis has to be done, so seized computer systems, in case of computer crime the crime scene, have to be examined for digital evidence. Several questions have to be answered, e.g. what has happened to the system since the computer was attacked. The investigators should try to reveal when and which event occurred. Also the method of attack should be discovered, as this could be another clue to describe the attacker's MO, and also gives input for a risk analysis that helps to prevent further attacks. As a second step, the investigators need to provide details for the victimology. The investigators should get an idea of the victim, the victims function, activity and awareness of computer security. All those gathered information needs to be bundled in the third part, the crime scene analysis, to get a more comprehensive picture of the perpetration of that crime. That picture, together with specific expert knowledge, experience gathered by observations or generalisations provided by the inductive profiling method can help to develop an attacker profile.

ISBN: 87-987271-6-8

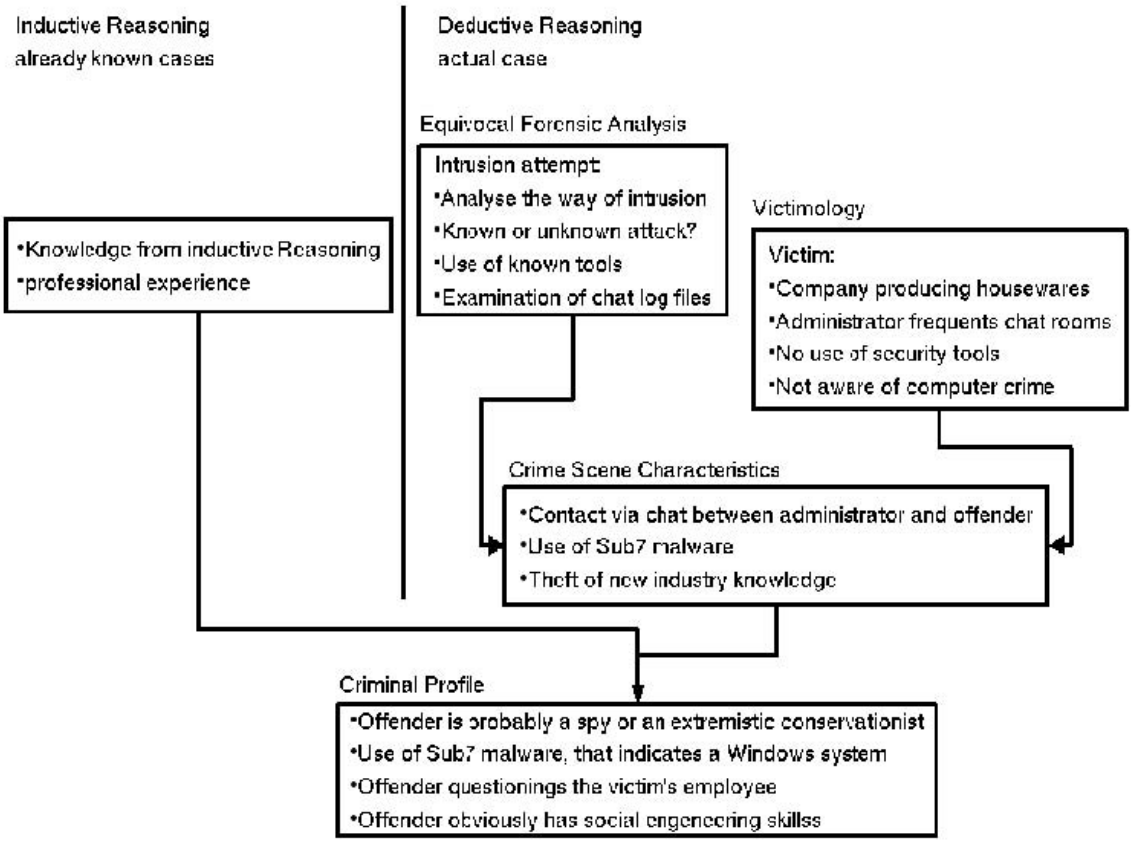

Figure 1. The Behavioural Evidence Analysis approach applied to computer crime.

The reasoning itself is very similar to the traditional profiling methods. The analysis results can show characteristics of the perpetrator in the same manner as for non-computer crime. The perpetrator's skills could be classified whether he/she uses special but public tools, or whether it seems that handmade tools are in use. In addition, log files can reveal whether or not the perpetrator is a Unix guru, having an excellent knowledge of the file system structure and commands, or a comparative novice. Performing computer forensics can also help to find indicators of whether the perpetrator comes from the outside, without special knowledge about the company or organisation structure and security mechanisms, or is an insider such as an employee. The review of a shell history file, which shows a hacker who often mistypes can provide an assumption that the perpetrator is not very confident or is possibly dyslexic.

The victimology has to be done in a cooperative way. Information about the victim can be provided by gathering digital evidence, as well as by questioning the victim and assessing the victim’s environment in the traditional method.

The forensic analysis of the computer system may reveal important aspects about the victim as well. A perpetrator might have had contact to his victim by e-mail or chat clients, by traditional post with letters written on the victim's

ISBN: 87-987271-6-8

computer, or by phone with associated notes being made and saved on the victim's computer. This could help for victimology as well as for a better understanding of the perpetrator's behaviour.

The gathered information has now to be used to provide the crime scene characteristics. As described by Turvey (2003, pp. 41-42) it is possible to reveal the perpetrator's method of approach, the method of attack, the method of control and others. The forensic analysis can help to reveal things such as the method of attack. If the attacker compromised the system without probing, but with several attacks in a specific order, this could show a modus operandi (MO) of his way to commit a crime.

An offender that just needs the computer to commit a crime, e.g. (cyber) stalking, needs to start his conversation or his contact with his victim in a special way, and he probably also meets only victims in cyberspace, that are similar in some way. This could also provide a hypothesis for the MO. In a stalking case, the way the offender and the victim are communicating, could reveal signature behaviour, for example if the offender has control over his victim in a very unusual way.

The creation of a timeline can help to understand the perpetrator's preferences to work on his crime. It can also offer clues to the perpetrator's location and/or his social origin. If the perpetrator is, during the week, mostly active late at night it could be assumed, that he or she is working during the day time, so the perpetrator is probably out of his teens. If the perpetrator is often active during day time, it could be possible that the perpetrator goes still to school or university. If the attack occurs multiple times, it is probably possible to trace back the attackers connection or, if the IP address is not spoofed and no or only compromised systems are involved, to identify the perpetrator's location, where he or she starts the attacks. This could help to the above described assumptions more clear, than by only reviewing the timeline.

The above examples suggest that an adaptation of existing profiling methods to the area of computer crimes is possible. If approached as indicated, these methods could be of value for law enforcement agencies, for investigating unknown computer criminals, as well as for risk analysis or assessment.

Discussion and Conclusion

This paper had outlined two approaches to profiling, namely the inductive and the deductive methods. Both are approved methods for criminal profiling in the general context. The initial question was, whether or not such methods can also be used to develop profiles for computer criminals. This question has been positively answered.

The inductive profiling method can be used whether there are a large volume of criminal cases, all related to the same kind of crime (e.g. cyber stalking). In this

ISBN: 87-987271-6-8

context, meaningful profiles can result only from relevant (i.e. separating between profiles) attributes that are analysed in a representative sample.

The inductive profiling has the potential to help in identifying affinities between different crimes of a specific type, which can, in some cases, reveal serial offenders. Inductive profiling can also give the investigators an idea of who they are looking for. Therefore inductive profile is often used as a generalisation about the characteristics of offenders of a specific crime (Turvey, 2003 p. 26).

Some of the principal taxonomies that we have uncovered, although potentially based upon sound evidence, do not publish details of the underlying data. As such, we intend to conduct our own survey as part of the ongoing research in order to enable suitable empirical data to be collected.

As the quality of an inductive profile depends on the existence of adequate data, it seems to be inappropriate to rely exclusively upon this method for law enforcement work against computer crime. The deductive profiling instead, offers the possibility to develop offender profiles that provide clues to the investigators, without being in need of a representative sample. In addition, unlike the inductive profile, the deductive profile informs the investigators about every footprint that the offender's activity caused.

The mechanisms are an important consideration for the deductive profiling method that can be used in extracting the digital footprints. Also important is the technology that enables one to create network footprints in a way that also maintains privacy protection. These issues will receive focus as part of our future work.

More generally, the ongoing research will focus upon the design, development and evaluation of a comprehensive profiling method, which enables the technical and psychological aspects to be combined and utilised within a coherent overall profile. A subset of representative cybercrime categories will be selected for detailed evaluation, and associated profiles will be developed, based upon a novel combination of methods identified here. Strategies will then be designed to facilitate the use of these profiles in the context of investigating, preventing, detecting, and responding to such incidents. This will involve the proposal of new methods for cybercrime investigators (e.g. use of the profiles in computer forensics), as well as means by which they can be automatically utilised within software systems for intrusion detection and response. The latter aspect will involve prototype software implementation of methods to formulate and utilise the profiles.

ISBN: 87-987271-6-8

References

Baurmann M. C. (2003) Die Operative Fallanalyse des Bundeskriminalamtes IN: Lorei C.ed. Polizei & Psychologie: Kongressband der Tagung "Polizei und Psychologie" am 18.und 19. März 2003 in Frankfurt am Main, Frankfurt / Germany, Verlag für Polizeiwissenschaft

Brock P. (1999) Spuren, die zum Charakter des Mörders führen, an Interview with Thomas Müller – Psychologist/Profiler, http://www.criminalprofiling.ch/methodmueller.html

Bundeskriminalamt (1999), http://www.bka.de/pks/pks1999/index2.html, last access11/03/2004

Bundeskriminalamt (2001), http://www.bka.de/pks/pks2001/p_3_21.pdf, last access11/03/2004

Canter D., Myers B.(1998), a radio interview from BBC 4, http://www.i-psy.com/publications/radio_four.php, last access 11/03/2004

Casey E. (2002) Handbook of Computer Crime Investigation, London, Academic Press

Casey E., Larson T. & Morrow Long H. (2002) Network Analysis IN: Casey E. ed. Handbook of Computer Crime Investigation, London Academic Press
CERT (2004) CERT/CC Statistics 1988-2003, http://www.cert.org/stats/, last access 11/03/2004

Dern H., Witt R. (2002) Operative Fallanalyse bei Tötungsdelikten IN: Egg R. ed. Tötungsdelikte: mediale Wahrnehmung, kriminologische Erkenntnisse, juristischeAufarbeitung, Wiesbaden / Germany, KrimZ Kriminologische Zentralstelle e.V.

Douglas J. E., Munn C. M. (1992) Modus Operandi and the Signature Aspects of Violent Crime IN: Douglas J. E., Burgess A. W., Burgess A. G., Ressler R. K., Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crimes, New York /U.S.A., Lexington Books

Furnell S. (2002), Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare*, vol. 1, no. 2. 35-44.

Halleck G. (1999), A Hacker Taxonomy, http://www.deaddrop.org/security/Papers/HackerTaxonomy.html, last access 11/03/2004

ISBN: 87-987271-6-8

Hammond S. (1999) Offender Profiling Of Sexual Offences, http://www.ramas.co.uk/offender_prof.pdf, last access 11/03/2004

Hoffmann J., Musolff C. (2000) Fallanalysen und Täterprofile, Wiesbaden, Bundeskriminalamt

Holmes Ronald M., Holmes Stephen T. (2002) Profiling Violent Crimes: An Investigative Tool, Third Edition, Thousand Oaks CA, SAGE Publications

Howard J. D., Longstaff T. A. (1998) A Common Language for Computer Security Incidents, http://www.cert.org/research/taxonomy_988667.pdf, last access 11/03/2004

Icove D., Seger K., VonStorch W. (1995) Computer Crime: A Crimefighter's Handbook, Sebastopol CA USA, O'Reilly & Associates Inc.

Musolff C. (2002) Täterprofile und Fallanalyse: Eine Bestandsaufnahme IN: Hoffmann J., Musolff C. eds. Täterprofile bei Gewaltverbrechen, Berlin Heidelberg, Springer

Noblett M. G., Pollitt M. M., Presley L. A. (2000) Recovering and Examining Computer Forensic Evidence, http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm, last access 11/03/2004

Petherick W. (1999) History and Application of Criminal Profiling, http://www.crimelibrary.com/criminology/criminalprofiling2/, last access 11/03/2004

Turvey B. (2003) Criminal Profiling: An Introduction To Behavioral Evidence Analysis,Second Edition, London San Diego, Academic Press

Schwartau W. (2000) Cyber Shock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption, New York, Thunder's Mouth Press

ISBN: 87-987271-6-8