J Comput Virol (2007) 3:135–141
DOI 10.1007/s11416-007-0042-4

Considering the potential of criminal profiling to combat hacking

Jörg Preuß · Steven M. Furnell · Maria Papadaki

Received: 12 January 2007 / Accepted: 11 March 2007 / Published online: 12 April 2007

Abstract This paper outlines the results of a case study focusing upon hacking incidents in Germany. This work aims to identify behavioural aspects of hackers and their motives for the development of a Criminal Profile. Therefore cases of hacking incidents have been studied to find commonalities and differences for motives, as well as the Modus Operandi (MO). Cases that have been observed within this study are those in which the perpetrator had been identified in person. All cases have been provided by the Bundeskriminalamt (German Federal Criminal Police Office). A total of 12 cases are analysed, revealing a number of common traits in terms of hacker activity and the methods used. This study indicates that methods which have already been used years ago are still preferred methods today. In ten out of twelve cases the observed characteristics fit within in the stereotype of a Script Kiddie. Only two hackers differed regarding their motives compared to the Script Kiddie hackers, but a significant difference regarding their methods—the MO—could not be noticed. From the twelve cases under investigation a basic principle could be identified: the hackers take the path of the least effort. This reveals a clue for the fact that a different motive does not necessarily lead to different methods.

1 Introduction

Hackers and their characteristics are often described with stereotypes like script kiddie, black hat, white hat and others [15]. Other variants of typology distinguish between crackers, criminals and vandals [9]. For the prosecutors both types of categorising provide no benefit in actually fighting cyber crime. A benefit could be to use knowledge about the attacker's aims, the methods and insights into demographic aspects, which might help by revealing clues for analysing the digital evidence. One method to achieve this comprehensive knowledge is Criminal Profiling [13], which represents a long-term known technique to overcome several types of crime. Different methods are used to develop a profile, some of which focus upon the development of a profile, whereas others focus upon the comprehensive understanding of the course of events that lead to the crime scene, the modus operandi (MO). For those methods the development of a profile is typically subordinated.

The methods for profile development are usual scientific methods, namely inductive and deductive reasoning [13]. The inductive reasoning approach leads to a generalisation, a profile of the typical criminal for the observed type of crime—a picture of a generalised perpetrator. In deductive reasoning, the research for a specific case, tries to draw a detailed picture of a concrete crime scene [18]. Insights gained by using one method can of course be used as input for the other method. For example, the knowledge of a general offender can be used as an anchor point or pivot element for a first crime scene analysis.

The research is limited to computer-focused crime, where the crime emerged as a direct result of computer technology and there is no direct parallel in other sectors [7]. The differences in computer crime will be distinguished according to the following paragraphs of the StGB (German Crime Law):

- § 202a StGB: Espionage (e.g. sniffing, reading data with Trojan).

J. Preuß (✉) · S. M. Furnell · M. Papadaki
Network Research Group, School of Computing,
Communications & Electronics, University of Plymouth,
Drake Circus, Plymouth PL4 8AA, UK
e-mail: joerg@preuss.info

- § 303a StGB: Illegal data modification (e.g. deletion of data).
- § 303b StGB: Computer sabotage (e.g. DDoS attack).

Although these paragraphs do not explicitly distinguish between computer-assisted and computer-focused crime, the different flavours of hacking (in respect of the different motivations) are suitably encompassed. Hacking itself is one typical computer-focused crime.

2 Hypotheses

The three assumptions for this work were formulated as hypotheses, which were then used as the basis for an analysis of known hacking cases. These hypotheses, and the thoughts that led to them, are detailed below.

2.1 H1: Perpetrators of different types of computer crime use different attack methods

This hypothesis is based on the fact that the law, which is focused, describes different types of crime. For an espionage attack it is necessary to gain information from the attacked system or systems beyond the attacked one. This means any kind of intrusion, being performed manually or automatically. A relatively recent variant of espionage is Phishing, where an offender tries to trick the potential victim, typically via e-mail, to use a fake site for entering personal data (e.g. bank account and PIN numbers) [12].

A sabotage does not necessarily need an intrusion. A typical sabotage act, the (Distributed) Denial of Service (DDoS) attack, can be performed by attacking vulnerabilities, which may crash a system or impair particular services. Other methods can also be used for computer sabotage, such as entering a system and stopping a service, or deleting material from the hard disk.

For the illegal modification it can be necessary to enter a system. It is also possible without any intrusion but using a Web-form with stolen credentials to modify data or using methods like cross site scripting (XSS) or Code Injection [12].

This considerations outline that nearly any technique could be used to commit each of those three types of crime. However, assuming that one is taking the path of the least resistance (if there is no reason for more sophisticated methods), the research will show that the type of crime, respective the perpetrator's motivation, can be determined by identifying the modus operandi (MO). That assumption, hackers are taking the path of least resistance, might be a correct one as Arnone [1] indicates. It is also known by other type of crimes like burglary, that perpetrators typically break into less secured houses, that can be entered without too much effort [11].

2.2 H2: Those different attack methods are distinguishable using intrusion detection systems and methods of computer forensics

This is based on the idea that intrusion detection systems (IDS), such as Snort (http://www.snort.org), are able to identify the type of attack using pattern recognition. The result of hacker profiles might lead to a classification of known IDS patterns.

Because of the same consideration made for H1, that an attacker takes the path of least effort, it can be assumed that the attackers will use mostly common and well-known exploits to reach their goal. Identifying so called zero day exploits might be a perfect way to successfully attack a system, because an administrator can hardly secure the systems against a threat which is not known during the time of attack. On the other hand identifying zero day exploits is not done without significant effort on the part of the hacker.

Well known exploits are published not only around the black hat community. They are also published via any information service in the Internet (e.g. Heise in Germany, ZDNet, etc.) or at security sites like e.g. SecurityFocus.com. Sometimes not only the idea behind the exploit is published but also the exploit code, sometimes pseudo-code sometimes real code. Some penetration testing tools, which are freely distributed as open source projects (e.g. Metasploit.org) provide one with ready implemented exploits and payloads.

So it is easier to use known exploits, even if several systems will be patched and thus no longer vulnerable. If hypothesis H1 indicates that differences in perpetration can give a hint who is attacking, H2 will outline whether this theoretical knowledge can be implemented in a technical way.

2.3 H3: The use of different attack methods relates to the attackers social situation and his level of education

The third hypothesis H3 is based on the assumption that there must be a relation between the perpetrator's social situation, their educational level and the methods used for the attack. This work tries to identify whether the technical methods or skills correlate to the perpetrator's educational level or other demographical parameters such as ethnic background.

It can be assumed that the educational level might influence the intensity of interest in technical details of computing and hacking. Meanwhile, the ethnic background might influence the possibilities for the development of skills and technical know how. The PISA study in 2000 from the OECD [2] outlines, that children of deprived families have more often a lower educational level than children from privileged families, so did UNICEF [19] and Bundesregierung [5]. Those disadvantages in education might lead to fewer chances for any kind of development—including the development of information technology knowledge.

3 Process of data gathering

In order to explore the hypotheses it was necessary to consider several methods of data gathering. The required details included both technical data, which could be fetched using intrusion detection systems or honeynets, and demographic information about the perpetrators. It was considered that the latter could potentially allow relations to be drawn between the modus operandi and the hacker as a person. This consideration led to the idea to develop a survey that contains questions about the hackers personality as well as their methodology [3].

A requirement for this survey was the validity of the gathered data. A survey distributed via Internet was ruled out because it would be virtually impossible to verify the results. As such, the chosen method for gathering data was a study of law enforcement files sourced from the Bundeskriminalamt. In order to avoid placing an undue burden upon active police officers, the files were studied, and the questionnaire completed, by ourselves. This also had the advantage, that there have not been any influences during ticking answers due to different levels of knowledge of each police officer. When the files level of detail has not been sufficient, responsible police officers have been interviewed to gain more details.

Only cases which provided enough information about demographic aspects as well as the modus operandi had been used, and in most cases the perpetrator had been sentenced. Another selection criteria had been the phenomenological aspect of the case. Only hacking cases have been examined. Phishing, developing and spreading dialers, and the distribution of illegal material have not been included within this work. Even though those types of crime may include a hacking component its role is incidental and the typical focus of investigation in those cases is the bribery or the illegal material itself (e.g. child porn), but not the hacking.

4 Survey summary

The research brought up twelve cases. during the years 1998 and 2004, which provided enough information for this questionnaire. Although criminal statistics suggested a mass of computer crime cases during this period, most dealt with warez, child porn, dialer and (for the newest cases) phishing, rather than hacking in its purest form. Nevertheless those twelve examined cases are documented very detailed for this research. At this point it can be observed that one result of this survey is, that law enforcement files are not the perfect input for this kind of research. The reason for this might be, that it is not necessary to reveal any information, that is addressed by the questionnaire, to convict a perpetrator. Another reason could be that many information are hard to gain afterwards. Only the interview of the perpetrator might provide deeper and detailed information, assumed the perpetrator is cooperative and truthfully reports.

It is important to mention that it is not possible to generalise, to develop a profile, with this small amount of cases. Conclusions can only be drawn for this sample and will be outlined in a descriptive way.

4.1 The standard hacker

Because it is not possible to develop a serious profile with a sample as small like this the picture of a standard hacker that is drawn in this section is restricted to the scope of the cases studied and should not be generalised to other cases.

Demographic attributes of the standard hacker are as following:

- The standard hacker is male and between his late teens and his early twenties. Two out of 12 hackers had been nearly 18 years old, four had been between 18 and 20 years old and two had been between 20 and 22 years old.
- The average hacker lives at his parents home and is still a student (secondary school or further education).

None demographic attributes that describe the standard hacker are:

- The operating systems used by the typical hacker are Windows (in all flavours 95,98,NT,2000,XP) and Linux.
- The standard motives are based upon financial reasons, fun and intellectual curiosity. Looking behind the tick boxes and the results, the motive of financial reasons can be split in two directions. The first is that a perpetrator wanted to have Internet access without paying for it. This flavour occurred for playing online games as well as staying operator of an IRC channel, which particularly means running one or more bots. The second flavour of financial reasons was earning money (e.g. due to selling warez).
- Both types of motive fun and intellectual curiosity occurred together. It was not possible to distinguish between both types for these twelve cases.
- The standard hacker attacks private persons, companies or educational organisations in an equal measure. Typically no indicators could be found out why the hacker had chosen a person in one case and a company in another case. This makes sense because of the above mentioned fact that a serious aim is gaining lots of zombie PC’s. It is not necessary for the perpetrator to address a specific system, but the mass of compromised and remote controlled systems is the big goal. This goal is identical to that of the herder of one or more Botnets today. As it can be assumed for the outlined victims the standard hacker attacks most common systems – namely Linux and Windows.

- The average hacker publishes or communicates details of his activity. This was done via IRC (Internet Relay Chat) in each of the investigated cases, a perpetrator did publish information.
- The attack is planned using port scans - seven of twelve did so. No details are known about the exact technique to scan open ports and find out vulnerabilities. Also no details are known whether the hacker did search for a specific vulnerability or not.
- Perpetrators typically performed attacks from their own systems or with one compromised system in between.
- Sabotage was a characteristic in 8 of twelve cases. In 6 cases this sabotage was not directed to a specific service, but the system as a whole, not caring which attacked service ties the system down. In five of these cases DoS or DDoS attacks were used.
- In all cases the hacker had entered the system and used the Internet as the entry point for his attack, rather than via a dial-in connection or physical access.
- In nine cases, the intrusion was realised via an attack against a vulnerable system. In one case phone phreaking was used to use the Internet for attacks without having costs and to cover the attacks.
- The standard hacker uses malware for his activities – in 8 of twelve cases. The type of malware is not known in detail, but the portfolio typically includes Trojans and Rootkits.
- Only less is known about whether the hacker examined the system or not and also about the way of examination or exploring. In three of twelve cases, where it is known, the hacker searched for password files.
- Besides computer sabotage hackers did modify data in 6 of twelve cases. In three of those cases system configuration files have been modified.
- The standard hacker also explored the system to spy out data (eight of twelve cases). This was done manually, in absence of any special equipment.
- Typically the hacker uses the compromised system for his own purpose. This has been done in ten of twelve cases.
- The average hacker does not wipe his footprints on the compromised system (nine of twelve).

In summary it can be observed that these cases actually adhered closely to the traditional stereotype of a hacker, and that from a practical perspective the methods employed to achieve the attack were not particularly sophisticated.

4.2 Outliers

Although this sample is very small, there are still two cases which are different to the average. Those two outliers have still a lot of commonalities with the standard hacker, but considering the details differences can be found.

Blackmailer The first outlier who does not exactly fit into the picture of the standard hacker is a single male, who was slightly older than the others—he was between 21 and 29 years. This young male had further education but was out of work during commitment, seeking for a job.

His motive is driven be his unemployment. This perpetrator was blackmailing a company to get a job offer from the attacked company. He did also contact the victim due to this blackmailing, to press the job offer.

The blackmailer performed computer sabotage and intrusion as well. In difference to the standard hacker, this attacker used malware, a Worm, for his computer sabotage DDoS attacks, which was developed by himself. He used a traditional programming language, C/C++. The Botnet created by the worm was used for covered attacks.

To examine or explore the victims system, the hacker installed keylogger and backdoor tools. He was searching for password files and confidential content that he could use for blackmailing. The hacker used encrypted connections to communicate with the victims system.

The main difference of this hacker is, that he had a precise motive and a more sophisticated performance compared to the others. He was not driven by fun and curiosity or only as a secondary motive. The primary motive was a concrete goal for this hacker. Also the effort, the hacker invested, was obviously higher developing own malware than downloading and using e.g. SubSeven.

Hate driven hacker Another hacker that can be noticed as an outlier, is a young male in the ages from 14 to 17 years, who is living at his parents home and is still going to school. These characteristics are not different to the standard hacker.

The difference concerned his motive and his way to achieve his goal. His activity is driven by hate against a company. A more secondary motive and again very similar to the standard hacker was sharing games, videos and other software.

As the standard hacker this perpetrator was also using the IRC to talk about himself. Alike he was using Windows and Linux for his activity. His focused aims were Windows systems, which he needed to install malware for his DDoS plans against the hated company.

Similar to the Blackmailer the hate driven hacker was involved in the development of the worm he used. It is not exactly known, in contrast to the Blackmailer, whether the malware was developed by this hacker himself, only modified or the hacker have had simply contact to the real developer. But also this hacker had a concrete goal and had been more engaged as the standard hacker achieving his goal.

5 Answers to the hypotheses

Although the sample is very small it is still possible to give some consideration to the hypotheses in this context.

5.1 Different method for different types of crime

The hypothesis H1 claimed that different methods of hacking are used for different types of crime. While planning this study, the type of crime was attached to the German Crime Law. During the study of the law enforcement files it turned out that nearly every one of the three focused statutes have been realised in each case. In nine of twelve cases multiple statutes have been addressed.

Defining a type of crime using the phenomenological concept (e.g. hacking, phishing, file sharing, identity theft, etc.) instead of the statutes of the German Crime Law might not make any difference to this result. The twelve cases contained hacking, file sharing and identity theft as well. None of the studied cases focused upon only one type of crime. It has typically been a mixture of the possibilities like sharing illegal files, hacking a server for sharing purposes, or sabotage-related activity (e.g. DDoS).

Differences could be noticed when the hacker had a more specific motive in mind and where a system had been consequently been targeted for a reason, rather than being attacked in an opportunistic or indiscriminate manner. In these cases, the efforts to achieve a goal are higher than for the standard hacker.

5.2 Different methods are distinguishable

The hypothesis H2 claimed that the different attack methods are distinguishable using intrusion detection system (IDS) and established methods of computer forensics.

The hacker did use established exploits. No Zero Day exploits have been noticed for those twelve cases. In one case the hacker was caught because he used SubSeven, which was of course noticed by the antivirus application running at the victim's system.

The outlier cases used more sophisticated methods to achieve their aims, but even these could have been noticed using up to date rules for the IDS.

The study suggested that gathering data about activities on a compromised system was problematic, at least insofar as the law enforcement records contained no detailed information about the type of activity that took place. This might be due to hackers wiping *at least some of* their footprints, and indeed there was rarely any information available about this process. Attacked Linux or Unix systems offered more information to the investigators than Windows systems. The audit trails of syslogd and other daemons provide quite verbose and detailed output about the systems and the users activities.

5.3 Social situation, educational level and the used methods

In these twelve cases eight hackers had been students, visiting school. The type of school is not clearly known, but from the ages of the individuals concerned it could be assumed that it was mainly secondary school, with a minority in further education (e.g. A level or comparable). Only one hacker had been visiting a university/college but was expelled. One out of twelve had been out of employment and for two others their educational status has not been mentioned in the law enforcement records, that have been studied for this research.

No correlation or at least relation between the used methods and the hackers social situation can be indicated. For example, the blackmailer (one of the outliers) was out of work and even not engaged in an educational process (further education, college, etc.) and performed quite sophisticated activities. In comparison the hacker, who was drawn from University/College, already having further education, used IRC, flooder, bouncer and other software found in the wild. The youngest hacker (in the age range up to 13 years), did not differ in the methods he used, although he might have had a lack of education because of his age.

6 Observations from the study

The case study brought up several insights which will be explained in the following.

6.1 Small amount of cases

The initial idea for a profiling approach, the inductive way of reasoning and this study was based upon the assumption that there might be a huge amount of cases to work with. This assumption was generated due to the amount of cases stated in the German Police Crime Statistic for computer crime. In 2002 there had been 1,327 cases reported in relation to data modification and sabotage [4]. A detailed examination of these had shown that hacking (the phenomenon that was meant to be focus of this study) was only a minority in its pure form. Many cases have been seen regarding to the phenomenon of dialer distribution.

Another fact that leads to a small amount of documented cases is that not every perpetrator leaves enough footprints at the system to trace him back, thus limiting the number that law enforcement was able to pursue to this extent. In addition, of course, the crime needs to be reported to the police in the first place, and in some cases this will not happen. Considerations such as loss of image are probable reasons for organisations such as financial institutes not to report those cases [14]. Meanwhile, others might not even notice that they have been hacked.

The lead author is also aware from informal talks at a conference that many cases are handled by the victim and a lawyer in a civil process against the perpetrator. As a result there is no police involvement.

6.2 The traceable hacker

Not every hacker is traceable. A reason can be that hackers wipe their footprints. In three of twelve cases it is known for certain that the hackers did wipe (some of) their footprints, by modifying or removing the audit trail or piped the logging output into `/dev/null`. Wiping footprints can hinder the forensic analyst from finding hints about the hacker's source system and the Modus Operandi.

Another reason is the use of launch pads. Only three cases involved hackers attacking the victim's system directly from their own Internet connection. Typically they use other compromised systems as a proxy or a middleman to cover their origin. In this context Botnets are the best way for a covered attack. As mentioned above the Botnet offers a C&C environment where there is no need for a direct contact. Even the newer use of P2P technology for creating and running a Botnet makes it nearly impossible to trace back a perpetrator.

6.3 Path of least effort

As mentioned during the derivation of H1 the hackers might use the path of least effort, and the twelve cases examined certainly support this view. Although the outliers show a serious goal like blackmailing or hate, they still used common methods. They did not develop highly sophisticated and individual methods, trying to find out a specific exploit for their target. They used documented attacks that could have been found online.

Also the effort to stay hidden during their attack, referring to all twelve hackers, follows the principle of minimum costs and maximum results. Using Botnets or other launch pads with installed Trojans and Backdoors is a quite easy way to go. The costs for compromising a system with a Bot are not high. It does not matter which system is infected. It is only important that a huge amount of systems have been hijacked (e.g. for DDoS attacks or spam mailing).

6.4 A medium for all

A interesting fact (and also a commonality for all cases) is that IRC seems to be a key technology for hackers. Each of the observed hackers has used the IRC for some reason. All of them used it for their more private communication, some also used it for their criminal activity. Also many of those who used the IRC for their private activity, hacked systems to install IRC bots, to ensure that they remained as the channel operator. Another aspect of being the master of a herd of IRC bots had been the ability to start DDoS attacks against hated chat members, one who talked disliked content during a chat session or to use the power of thousands of zombie PC's for blackmailing or harming.

The medium IRC obviously also played a major role in the former community of black hats. Today IRC and bots are still used techniques for criminal activities, e.g. the basis for Phishing are botnets. Although today techniques are implemented to create botnets are changing from before IRC to P2P or a combination of both to offer Command and Control Channels (C&C) [6,8].

Another aspect for IRC bots is that tracking back the hacker's path is hardly possible. They command their bots via IRC chat, and do not need to contact the compromised systems directly. If needed, hackers can connect to a compromised system via pre installed backdoors, which can then be used as a launch pad for further activities. However, bots typically provide many features that can be triggered via the C&C channel, thus removing the need for direct interaction [10].

7 Conclusions

The study outlines the problematic of mass infection, using common, low-cost hacking methods. Today knowledge of malware usage for malicious activity shows that hacking itself seems to be more a minor problem. As long as unsecured systems are around and connected to the Internet as well as no valuable methods to fight Botnets exist there is no need for the blackhats to change their strategy and methods.

No final statement could be given regarding the basic idea behind this research: whether it is possible to adopt the methods of criminal profiling for hacker or not. As initially mentioned it is necessary to gather information using inductive reasoning for developing a basis profile. A mass of cases for the pure hacking could not be provided by law enforcement records. Possible reasons for this are:

- today's blackhats moved to more efficient and economic methods,
- loss of image for the victim—fighting cyber crime without exposure via the civil way,
- professional cyber crime can hardly be noticed.

Another aspect that should be considered is that a perpetrator has limited possibilities by which to perform his hacking compared to other criminal contexts, such as sexual violence crimes. For violent crimes the perpetrator is mainly limited by his mind, which potentially enables the profiler to identify him by finding links between his personality and his activity. However, for computer crimes, especially hacking, the perpetrator is limited by the computer system. An attack is only possible where a vulnerability exists. The type of vulnerability thus helps to define the process of exploitation, whereas the type of violence against a victim can vary nearly without any limitation but the perpetrator himself. The studied cases for this research do outline only the spectrum of hacking methods for a quite homogeneous field of motives. In absence of other motives it is not possible to say that the aforementioned assumption is proven by this research. An indication for this assumption is that no differences regarding the methods could be noticed between the first and the last observed case. This suggests that the assumption regarding the effort, but it also suggests that no other possibilities for hacking the systems existed to achieve the hacker's goals. Looking at the mass-phenomenon of Botnets, it becomes obvious that the methods that are used for gaining zombie PCs are typically very similar to the methods observed in this work. This shows that—over a longer period of time—there had been no necessity to develop completely new methods. As long as there is no reason for different methods, the common methods will continue to be used.

Again, in the context of the small size of the sample, there is no possibility to conclude in favour or against the adoption of criminal profiling to fight hacking or computer crime. The sample did only show a quite homogeneous field of perpetrators. As far as the law enforcement records were able to provide the information, the Modus Operandi did not differ significantly. Considering that the motives were also very homogeneous and that both the ‘standard hacker’ cases and the outliers seemed to fit the picture of a script kiddie, the adoption of criminal profiling amongst this sample would offer no advantage.

A deeper insight in the field of computer crime, preferably espionage rather than script kiddie activity, is necessary to find out more about the Modus Operandi and psychological aspects like the motives. Cases need to be observed where the value of the achievement is high enough to see highly sophisticated and expensive methods of perpetration. The process of gathering data has to be reconsidered. On the basis of the experience in this study, it seems that law enforcement records are not the most suitable source of information for this type of crime. An anonymous questionnaire addressed to potential civil victims (e.g. affiliated groups with distributed locations) might provide more useful results. Such a sample might be a much better input for profiling purposes, and from such a basis the value of a profiling approach for computer crime could then be more seriously discussed.

References

1. Arnone, M.: White hat, gray hat, black hat: Hackers can teach government and industry valuable IT security lessons, Retrieved 25 March 2007, from http://www.fcw.com/article90994-10-03-05-Print&printLayout (2005)
2. Artelt, C., Baumert, J., Klieme, E., Neubrand, M., Prenzel, M., Schiefele, U., Schneider, W., Schümer, G., Stanat, P., Tillmann, K.-J., Weiß, M.: PISA 2000: Zusammenfassung zentraler Befunde, Retrieved 28 December 2006 (2001) from http://www.pisa.oecd.org/dataoecd/30/63/33684930.pdf
3. Buckingham, A., Saunders, P.: The Survey Methods Workbook: from Design to Analysis. Polity Press, Cambridge (2004)
4. Bundeskriminalamt: Police Crime Statistics 2002: Federal Republic of Germany, Retrieved 27 December 2006 from http://www.bundeskriminalamt.de/pks/pks2002ev/pcs_2002.pdf
5. Bundesregierung: Lebenslagen in Deutschland: Der 2. Armutsbericht er Bundesregierung—Kurzfassung, Retrieved 5 January 2007 (2005) from http://www.bmas.bund.de/BMAS/Redaktion/Pdf/Publikationen/Armuts-und-Reichtumsbericht/armuts-und-reichtumsbericht-der-bundesregierung-2-kurz,property=pdf,bereich=bmas,sprache=de,rwb=true.pdf
6. Fendley, S.: As the Bot Turns, Retrieved 11 November 2006, from http://isc.sans.org/diary.php?storyid=1300&isc=c294fbd688efb0822d11c9a0c02d0583
7. Furnell, S.M.: The problem of categorising cybercrime and cybercriminals. In: Proceedings of the 2nd Australian Information Warfare and Security Conference, Perth, Western Australia, 29–30 November 2001
8. Holz, T.: A Short Visit to the Bot Zoo, Retrieved 11 November 2006 (2005) from http://pi1.informatik.uni-mannheim.de/publications/show/13
9. Icove, D., Seger, K., VonStorch, W.: Computer Crime: A Crimefighter's Handbook. O'Reilly & Associates, Sebastopol (1995)
10. Lurhq: Phatbot Trojan Analysis, Retrieved 11 November 2006 (2004) from http://www.lurhq.com/phatbot.html
11. Meyr, J.: Wohnungseinbruch in München, Kriminalistik, no. 2, pp. 118–120. Kriminalistik Verlag, Heidelberg (2006)
12. Ollmann, G.: HTML Code Injection and Cross-site Scripting, Retrieved 3 December 2006 (2003) from http://www.technicalinfo.net/papers/CSS.html
13. Preuss, J., Furnell, S.M., Lea, S.J.: Research in Progress Paper, The Adoption of Criminal Profiling for Computer Crime. In: Gattiker, U.E. (ed.), EICAR 2004 Conference CD-rom: Best Paper Proceedings (ISBN: 87-987271-6-8), EICAR e.V., Copenhagen, 16 p (2004)
14. Schultz, A.: Neue Strafbarkeiten und Probleme—Der Entwurf des Strafrechtsänderungsgesetzes (StrafÄndG) zur Bekämpfung der Computerkriminalität vom 20.09.2006, Retrieved 17 November 2006, from http://www.medien-internet -und-recht.de/volltext.php? mir_dok_id=398
15. Schwartau, W.: Cybershock. Thunder's Mouth Press, New York (2000)
16. Taylor, P.: Hackers: Crime in the Digital Sublime. Routledge, New York (1999)
17. Turkle, S.: Life on the Screen: Identity in the Age of the Internet. Touchstone, New York (1995)
18. Turvey B.: Criminal profiling: an introduction to behavioral evidence analysis, 2nd edn. Academic, London (2003)
19. UNICEF.: A League Table of Educational Disadvantage in Rich Nations, Retrieved 28 December 2006 (2002) from http://www.unicef-icdc.org/publications/pdf/repcard4e.pdf