PAPER:

MODELS OF INVESTIGATION AND PROCESSING OF DIGITAL EVIDENCE

By **Zdeněk Blažek,** PhD, CISM

Introduction

This paper describes, in brief, some of the problems related to human behavior in cyberspace, possible new crimes, the collection of digital data for the purposes of evidence, and the archiving of digital data. In a big organization, it is possible to see the results of unlimited human behaviour on world network space – the internet. Current efforts to control this environment are far from successful, in particular the struggle against anti-social activities, as well as for the collection and archiving of data. It has to be recognized that the application of laws in relation to the internet are contradictory. Single governments attempt to limit criminal activities on the internet, but the results are not, and cannot be satisfactory. The reasons include: lack of unity, legal incompatibility, different goals, and the possibilities and sometime wishes of some governments to use the internet as a battlefield. A significant problem for organizations is the drafting of laws that do not take into account the consequences that follow. An example is the law passed in Germany, Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG),[1] especially the provisions of section 202c, which reads (Section 202a is presented because section 202c refers to section 202c):

> § 202a Ausspähen von Daten
> (1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
> (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202a Data espionage
(1) Whosoever, without authorisation, obtains access to data for himself or another, which is not intended for him and which was protected against unauthorized access by overcoming the protection, shall be punished with a term of imprisonment of up to three years or with fine.
(2) Data in the sense of the Subsection (1) shall only be those that are stored or transmitted electronically or magnetically or otherwise in a manner that is not directly perceptible.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten
(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Straftat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 202c StGB The preparation of espionage and interception of data
(1) Whosoever prepares a criminal offence according to the terms of § 202a or § 202b by manufacturing, obtaining for himself or another,

[1] *Geltung ab 11.08.2007; G. v. 07.08.2007 BGBl. I S. 1786 (Amending Act to the criminal code to combat computer fraud (41. Amendatory act to the criminal code)) dated 7 August 2007, in force from 11.08.2007. Translation with the help of Dr Martin Eßer, a member of the Editorial Board of the Digital Evidence and Electronic Signature Law Review.*

When working as a standalone device, it can be a useful assistant for a person with mental problems, but when connected to a networked personal computer, it is possible to obtain another impression.

selling, providing access to others, distributing or otherwise making available

1. passwords or other security codes, which provide access to data (§ make 202a (2)), or
2. computer programs, which serve to commit such criminal offence, shall be punished with a fine or a custodial sentence of up to a year.

(2) § 149 Subsection 2 and 3 apply accordingly.

This law significantly reduced the scope of the work undertaken by IT security companies and experts, because they can be now punished as criminals if they use tools that may be used for crimes. Similar laws are also under preparation in a number of countries. It seems that such laws may be counter productive, because it is possible to use current laws with slight modifications and without the unwanted results.[2]

Human behavior in cyberspace

We can fully see the phenomenon of Dr. Jekyll and Mr. Hyde on the internet. What people cannot allow themselves to do in the physical world, they do over the internet without any inhibition. Examples include blogs and chat rooms in which people make outrageous statements about each other, use rude words, and indulge in virtual sex and such like; however, such behaviour cannot be considered to be correct.[3] This phenomenon desensitizes the person. As an example, we can demonstrate pilferage undertaken by game players. This pilferage is the theft of a player's accounts. When a person commits fraud in virtual reality, it is possible to be fraudulent in the physical world, and vice versa. These problems are far from being tackled. Games are played on black servers in countries out of our legal control; software is copied, as well as movies and music. In addition, virtual cities and lives are created, and a great deal can be found in this environment: murder, fraud and sex.

The possibility of new crimes

The market adopts new products whose effect on the lives of people cannot be fully estimated immediately. As an example, consider AVS (Audio Visual Stimulation) devices. When working as a standalone device, it can be a useful assistant for a person with mental problems, but when connected to a networked personal computer, it is possible to obtain another impression. It is possible to upload modified software which can evoke later, for example, an epileptic fit and mood change. It is possible to manually edit such programs or download them. These devices have an influence directly on brain waves, and so they have an influence on brain activity. When and if such devices exist and they are sold, it is to be expected that they will be misused. It is also possible to attack medical devices, such as remote robotic surgery. The first experiments were undertaken via highly secure optical links; later experiments were undertaken via virtual private networks over the internet by way of a common user carrier with a lower level of security. But internet lines can be attacked, for example by DDoS (Distributed Denial of Service), and the consequences can be serious for health and life. Hospital networks can be the target of external or internal attacks, just as the networks of other organizations, both public and private. There are good forensic techniques for the standard computer environment, but there are no procedures for non-typical medical devices, where non-standard operating systems are installed with non-standard peripherals.

Models and guidelines for first responders

The police are very often in a position of a passive witness, because of the higher volumes of the use of modern technology. It is almost impossible for a single person to be familiar with every electronic device currently in use. The other problem is a shortage of highly qualified staff; people who know where to look

[2] *For a number of articles on this topic, see http://www.zdnet.co.uk/tsearch/uk+hi+cybercrime.htm.*

[4] *For instance, see MUDr. Karel Nešpor, CSc., PhDr. Ladislav Csémy, Zdravotní rizika počítačových her a videoher, 14.11.2007 (Health risks of computer games and video games), available at http://www.babinet.cz/podlupou.php?id=3813.*

for evidence and how to secure it.[4] The other very important point is that very often law enforcement units do not recognize that criminals are ahead of them and sometime their actions cause fatal mistakes.[5] This means there is a need to focus on guidelines or models and procedures for law enforcement units. Some guidelines have already been prepared.[6] The guidelines for police staff include the following trends:

1. The authors of guidelines are experienced policemen who are also familiar with digital evidence specialists. This is illustrated in the inclusion of such topics as the general seizure of evidence, which means that, for example, fingerprints and other classical evidence must be taken into consideration - so it is necessary to protect the keyboard and other peripheral devices, which a lay person may not consider necessary. This is because some chemicals used during the seizure process can destroy electronic equipment.
2. Although the authors tend to be experienced digital evidence specialists, the material does not appear to be prepared in close cooperation with experienced policemen. This means that such guidance is focused on IT problems and set-up procedures when investigating electronic devices, but omits to consider that there can be valuable evidence on other devices which can be very important, for example, to discover an identity of the last user.
3. A common attribute of nearly all the guidelines is an absence of technological procedures. For instance, it means that memory cards should not be exposed to an electrostatic field, or low temperature (frost can reliably erase data stored on electronic devices; for instance, codes in car radios are possible to erase by a short period of time in a freezer: -10°C is sufficient).

Guidelines, especially for first responders, might usefully be created in combination with the police, digital evidence specialists and technology experts.[7] Out of necessity, such procedures must be monitored and regularly updated. In my experience, it is necessary in the case of an action within a company, that it is essential that a digital evidence specialist will be on site to save evidence with minimum effect on the daily business.

The importance of digital evidence cannot be over estimated. Digital evidence can provide a lead to other evidence, and can corroborate other forms of evidence. Digital evidence can be direct evidence, such as documents or traces of internet activity, if the evidence is well documented and directly related to the person under suspicion or the company. Such digital evidence must be seized in a manner that is legally acceptable and with the minimum amount of changes. Where evidence is altered, any changes must be accounted for. It is necessary to prove that the evidence is identical to what was received, and the analysis should be repeatable. This means that the entire process must be carried out to achieve maximum credibility from the point of view of data collection, storing, analysis and must be repeatable. Results obtained must be translated into a language that is easily understandable for the lay person. The presentation itself must also be easy to understand and without loss of important data.

Identifying the user identification

Digital evidence is often a relationship between the evidence and a person or a number of people. This relationship is not close, and so the credibility of the evidence of linking a person to a particular act or document can be low. It is usual for the link between identifying the user of a computer or device and the person that was actually responsible for the action is not very strong, especially on home PCs. For example, e-mail boxes that can be viewed via a web interface can be, and are modified. This means it is difficult to guarantee the content of an e-mail. Hackers can penetrate computers by using malicious software and obtain access to mailboxes and other places without any knowledge of the owner or user of a PC. This means the credibility of digital evidence can be decreased very

[4] *See, for example, Andy McCue, ' Police forces lack e-crime expertise and resources' , Silicon.com, 18 March 2008 10:00 GMT, http://www.silicon.com/ciojury/0,3800003161,39170382,00.htm.*

[5] *Další zbraň proti bossu Starkovi – hacker, 20. listopadu 2007 1:39 (Another weapon against boss Starka - hacker) at http://zpravy.idnes.cz/dalsi-zbran-proti-bossu-starkovi-hacker-f08-/krimi.asp?c=A071119_215401_krimi_mia; for a list of article relating to hacking, see http://www.krab.cz/index.php?co_je=hacker%20%5Bhekr%5D.*

[6] *See the most recent version of the English police guide, Good Practice Guide for Computer Based Electronic Evidence (Association of Chief Police Officers, 2008), http://www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf; NIJ Special report, Forensic Examination of Digital Evidence, A Guide for Law Enforcement (US Department of Justice, Office of Justice Program, National Institute of Justice, April 2004), http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm; K M Waggoner, editor, Handbook of Forensic Services (US Department of Justice, Federal Bureau of Investigation, Laboratory Division, 2007), http://www.fbi.gov/hq/lab/handbook/forensics.pdf; Guidelines for best practice in the forensic examination of digital technology (IOCE, May 2002), http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html.*

[7] *Although see Peter Sommer, Directors & Corporate Advisors' Guide to Digital Investigations and Evidence (IAAC, 2005), http://www.iaac.org.uk/Default.aspx?tabid=65 and Electronic Crime Scene Investigation: A Guide For First Responders (US Department of Justice, Office of Justice Program, July 2001), http://www.ncjrs.org/pdffiles1/nij/187736.pdf.*

simply. Generally, identity management is not a simple matter, and to establish a credible and provable authorization and authentication is a complex matter. Even biometric measurements are not reliable, because much depends on the type of sensor used. For instance, to obtain access to the system using a capacity based fingerprints sensor, it is often enough to simply breathe on the surface of the sensor. Even the use of a digital signature cannot be considered as perfectly reliable,[8] and a digital signature does not prove that the private key was actually used by the owner of the private key.

Digital evidence archiving

As with other paper documents, so it is necessary for an organization to archive digital documents. But there are some differences in the digital world. The archiving does not just mean the secure storage of data, but also the need to ensure data readability and accessibility. It very often means not only to maintain documents and other data, but also the application that makes it possible to obtain access to the data. This is a problem which is not easily solved and which will increasingly become problematic in the future. Archiving of digital evidence is mentioned in RFC 3227,[9] where the problem is treated in a perfunctory manner:

> 4.2 Where and how to Archive
>
> If possible commonly used media (rather than some obscure storage media) should be used for archiving.
>
> Access to evidence should be extremely restricted, and should be clearly documented. It should be possible to detect unauthorized access.

This description demonstrates the authors are not aware of the issues at all. There is a significant difference between using back-up tapes for the purposes of disaster recovery and the long term archiving of data. In my experience, on several occasions we have not been able, even after 10 years, to read data from old data carriers, such as 5.25 inch floppy disks and old tapes. It is necessary to adopt a systematic approach in this area, and there are only a few attempts to do some work in the field.[10] It is important to consider long term conservation of documents in digital format, both documents that are scanned versions of paper documents, and documents created in digital format, because laws and regulations require the retention of documents, such as data concerning employees and accounting papers. The amount of data is permanently increasing.[11] Sooner or later we will have to deal with the practical problem of how to read and maintain old digital data.

From the perspective of running a large organization, it is interesting to note how some companies selling storage solutions provide certificates claiming that the data stored on their devices will be retained for 100 years, but the reality shows that after three years, there are some problems with obtaining access to and reading data from such ‘certified’ carriers. In addition, standards are changing rapidly, and very often obsolete standards are very quickly forgotten and there is no hardware or software to enable data to be viewed and processed. But there are also other risks. Some applications use non-standard databases or other means to store data, and without the applications, the user is not able to obtain access to and read the data. And application problem is that applications usually depends on operating system. Within 10 years we change it roughly twice in our organization, so it can happen that an application will be incompatible with an operating system and we shall not be able to recover any data. Without a proper application, we would lose the ability to obtain access to data. In addition, it means that not only data but applications, too, can be a very important point in respect of archiving data.

The device also has an influence on archiving digital evidence. The US courts have already had to deal with such a problem, as in the case of *PHE, Incorporated dba Adam & Eve v Department of Justice*,[12] where PHE were ordered to review information contained in a database, even though no program existed to enable them to obtain the information requested by the Department of Justice.[13] The other risk is where data might be inadvertently destroyed when trying to reconstruct data. This leads to the conclusion that proper models and procedures will be helpful in how to maintain data for the future. Ideally, such models should be standardized and commonly usable.

[8] *V. Klíma, Hashovací funkce MD5 a další prolomeny, 25.8.2004 (Hash Function MD5 and Others - Broken), http://www.root.cz/clanky/hasovaci-funkce-md5-a-dalsi-prolomeny/nazory/39659/.*

[9] *http://www.ietf.org/rfc/rfc3227.txt.*

[10] *For a discussion of the problems in the legal context, Stephen Mason, Electronic Evidence: Disclosure, Discovery & Admissibility (LexisNexis Butterworths, 2007), 4.27-4.35, and for a list of organizations working on this problem see Stephen Mason, Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence (research paper for the ARMA Educational Foundation, 2006) http://armaedfoundation.org/2006research projects.html.*

[11] *For the most recent discussion, see John F. Gantz, project director, The Diverse and Expanding Digital Universe (IDC Research, March 2008), http://arstechnica.com/news.ars/post/20080312-study-amount-of-digital-info-global-storage-capacity.html.*

[12] *139 F.R.D. 249 (D.D.C. 1991).*

[13] *Stephen Mason, Electronic Evidence: Disclosure, Discovery & Admissibility (LexisNexis Butterworths, 2007), 2.05.*

As an example, please note part of the form used for evidence archiving in table 1. The form ought to be compiled by the lawyer and the IT specialist. We should know if it is possible to reconstruct such data, and how to reconstruct it. In addition, there are some documents with electronic signatures and must be readable and accessible in the future, if only because they are of higher importance.[14]

We have to decide now what to do with the vast amount of data we are accumulating, and the effect that a potential loss of data will have in the future. To finish, to use old Latin, 'Videant consules....' (.... Let the Consuls see to it that no harm befall the State).

Archiving of digital evidence				
Time period of data request	30 years	20 years	15 years	5 years
Risk rating if data is missing	Very High	High	Low	Minimum
Whether data is stored abroad	No	Yes	If yes, where?	
Whether a solution for archiving exists abroad	No	Yes	If yes, which one? Specify	
Whether a local solution exist for archiving	No	Yes	If yes, which one? Specify	
Data importance from historical point of view	High	Medium	Low	
Data importance from legal point of view	High	Medium	Low	

Table 1 **Part of a form accompanying the procedure for evidence archiving request**

Mr. Blazek was a member of the criminal court senate until 1994, and an assistant professor at the Czech Technical University until 1995 before joining Commerzbank AG as a Head of IT and IT Security Manager. He has also worked as an external consultant for National Semiconductor (USA) and other companies.

[14] *Stefanie Fischer-Dieskau and Daniel Wilke, ' Electronically signed documents: legal requirements and measures for their long-term conservation' , Digital Evidence and Electronic Signature Law Review, 3 (2006) 40 – 44.*