Report from Dagstuhl Seminar 13482

Forensic Computing

Edited by

Felix C. Freiling[1], Gerrit Hornung[2], and Radim Polcák[3]

1 Friedrich-Alexander-Universität Erlangen-Nürnberg, DE, felix.freiling@cs.fau.de
2 Universität Passau, DE, gerrit.hornung@uni-passau.de
3 Masaryk University, CZ

Abstract

Forensic computing (sometimes also called *digital forensics*, *computer forensics* or *IT forensics*) is a branch of forensic science pertaining to digital evidence, i.e., any legal evidence that is processed by digital computer systems or stored on digital storage media. Forensic computing is a new discipline evolving within the intersection of several established research areas such as computer science, computer engineering and law.

Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges.

This Dagstuhl seminar brought together researchers and practitioners from computer science and law covering the diverse areas of forensic computing. The goal of the seminar was to further establish forensic computing as a scientific research discipline, to identify the strengths and weaknesses of the research field, and to discuss the foundations of its methodology.

The seminar was jointly organized by Prof. Dr. Felix Freiling (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany), Prof. Dr. Radim Polčàk (Masaryk University, Czech Republic), Prof. Dr. Gerrit Hornung (Universität Passau, Germany). It was attended by 22 participants and its structure was based on experiences from a similar seminar in 2011 (Dagstuhl Seminar 11401).

Seminar 24.–29. Novermber, 2013 – www.dagstuhl.de/13482
1998 ACM Subject Classification D.4.6 Security and Protection, K.4.2 Social Issues, K.5.2 Governmental Issues
Keywords and phrases practical experience in forensics and law; applied forensic computing
Digital Object Identifier 10.4230/DagRep.3.11.193
Edited in cooperation with Michael Gruhn

1 Executive Summary

Felix C. Freiling
Radim Polcák
Gerrit Hornung

After a brief introduction by the organizers, the seminar started off with a sequence of 3 slide/5 minute talks by all participants stating their research interests, their background and their expectations towards the seminar. In the afternoon, three motivation talks by Felix Freiling ("What is forensic computing?"), Gerrit Hornung ("The fundamental rights dimension of individual and mass surveillance") and Radim Polčàk ("Experiences from drafting the cybersecurity act in CZ") paved the way for a common understanding of the open questions in the area and the relation of forensic computing to computer security law.

The rest of the afternoon questions and expectations were collected and grouped using moderation cards. The result was a spectrum of five areas of interest that we termed as follows:

1. technical possibilities for evidence collection
2. digital evidence: admissibility, spoofing, integrity protection
3. open source intelligence
4. investigations vs. privacy
5. offensive countermeasures
6. transborder/cloud evidence collection

For immediate discussion on Tuesday the participants voted for their favorite topics. As a result, three discussion groups were formed for the next day: digital evidence (topic 2), investigations vs. privacy (topic 4) and offensive countermeasures (topic 5). Topic 1 was to be handled by an overview talk by Andreas Dewald on the following day.

Tuesday morning started with a talk by Andreas Dewald on technically unavoidable evidence and was followed by a multimedia presentation about cold boot and hot re-plug attacks. After this technical introduction work in the discussion groups took place until the afternoon, when the collected results of the discussion groups were presented in a plenary session. As a highlight, the group on offensive countermeasures presented a taxonomy of 5 categories of offensive countermeasures that were specific enough for both law and computer science to investigate. The results of all discussion groups are summarized later in this report.

Wednesday morning commenced with a talk about the work of Interpol by Jan Ellermann ("Data protection as an asset in Europol's fight against cybercrime"). It was followed by a presentation of current research by Dominik Herrmann about the usage of fingerprinting in network forensics ("Fingerprinting Techniques for Network Forensics"). The round of talks was concluded by an introduction to the law of evidence in criminal procedural law by Tobias Singelstein ("Basics zum Beweisrecht im Strafverfahren").

The afternoon was spent on a pleasant hike to a nearby village where the Dagstuhl office had organized delicious traditional coffee and cake. On the way back to Schloss Dagstuhl a group of adventurers again, as in 2011, separated from the main party to explore the woods around Wadern. However, unlike 2011, they managed to return to Dagstuhl in time without major difficulties.

Thursday was started with a talk by Dennis Heinson on investigations in enterprises ("Internal Investigations, IT Forensics and Law"). Afterwards two new discussion groups were formed, partly based on the areas of interest collected on Monday, and commenced discussing the topics of (1) internal investigations and (2) transborder/cloud issues. In the afternoon, the results of these groups were collected in a plenary session during which especially the transboder issues caused a heated and insightful discussion.

Friday morning hosted a series of three talks from computer science, law and practice by Christian Hawellek (on techniques for modeling surveillance), Stefan Kiltz ("Forensically Sound Data for Digitised Forensics on the Example of Locksmith Forensics") and – last but not least – Erich Schweighofer ("Surveillance of US-surveillance").

Conclusion

In summary, the participants (and the organizers) enjoyed the week in Dagstuhl. In particular, the chance to get to know many new people from both the technical and the legal side of forensic computing was appreciated. From the viewpoint of the organizers, several points appear worth mentioning which we wish to document here.

First of all, it became clear to all participants that forensic computing is still in the process of maturing. The legal regulations as well as the technical instruments used in forensic computing are evolving quickly and it needs a joint effort by both communities to make progress. In our opinion, the seminar was much better than the preceding seminar in 2011, mainly because the lawyers were more interested in technical details and the technical people presented their "special secret instruments" in an understandable way. The seminar showed that fruitful discussions between both sides are possible, that lawyers can be cool as well and that there exist at least some lawyers with advanced technical understanding. For the technical people it was insightful to get a basic feeling on how the interpretation of law works and to see that there are quite a lot of gray legal areas. After all, forensic expertise is just one bit of evidence in court, and it may not be the most important one. And there are actually many, many data protection problems out there that will need to be handled within the field of forensic computing.

Overall, it was again a challenge to gather interested people in Dagstuhl. Dagstuhl seminars are well-known in computer science, but not in law, and it is well-known that practitioners, which are common in forensic computing (prosecutors, defenders, police, expert witnesses), with their tight time schedules can hardly afford to come to Dagstuhl for an entire week, especially from overseas. This is a problem which will remain and explains why – again – the seminar was dominated by German speaking participants.

The topic of forensic computing, however, is also gaining importance in the academic community, and at Dagstuhl: In February 2014, a seminar on "Digital Evidence and Forensic Readiness" (Dagstuhl Seminar 14092) will take place, opening the possibility for several of the participants to meet and discuss again, albeit with a slightly sharpened focus. In case another general seminar like this would take place, the topic of mutual understanding can be placed into focus even stronger. This could be achieved by distributing introductory papers from "the other side" in advance or by giving introductory tutorials in forensic techniques at the seminar. In the end, the seminar left us with more open questions than we had at the beginning. But at least this was to be expected.

2 Table of Contents

Executive Summary

Overview of Talks

Discussion Groups

3 Overview of Talks

3.1 Technically Unavoidable Evidence

Andreas Dewald (Friedrich-Alexander-Universität Erlangen-Nürnberg, DE)

A common question in forensic computing is the following: Looking at a seized hard drive, which actions have been performed by the user? To answer this question, the forensic expert needs to analyze digital evidence and finally presented it in court. But which evidence is good evidence? How meaningful is it? How convincing? The probably most important distinction regarding this questions is the notion of technically avoidable and unavoidable evidence. Technically avoidable evidence is data that is generated for its own sake and can easily be avoided, such as document files, for example. Technically unavoidable evidence in contrast is data that is unintentionally (and most times unknowingly) generated by the system and cannot be configured away – at least not by a "normal" user. Even though this definition strongly depends on the perception of what the user is able to do, technically unavoidable evidence has a high probative value in general. As an example of such evidence, we present the concept of application fingerprinting based on filesystem timestamps: We found that on any action performed by a user (like sending an email or browsing a website) timestamps of various files are changed in a characteristic way. Those "fingerprints" in timestamp data are a good example for technically unavoidable evidence with high probative value. In this case, the extraction of the evidence even can be highly automated to support the investigation with a quick overview of known actions that happened lately.

3.2 Data protection as an asset in Europol's fight against cybercrime

Jan Ellermann (Europol, NL)

Joint work of Ellermann, Jan; Drewer, Daniel
Main reference D. Drewer, J. Ellermann, "Europol's data protection framework as an asset in the fight against cybercrime," ERA Forum, 13(3):381–395, 2012.
URL http://dx.doi.org/10.1007/s12027-012-0268-6

The European Union has launched its own European Cybercrime Centre (EC3) at the beginning of 2013. A related feasibility study carried out for the European Commission reveals that next to operational considerations strong data protection safeguards constitute one of the main factors for having the centre hosted at the European Police Office (Europol). Data protection and the fight against cybercrime do certainly not constitute a contradiction. On the contrary, due protection of information relating to identified or identifiable natural persons is a prerequisite to prevent identity theft and other forms of cybercrime.

The talk I have given has illustrated the solid data protection regime at Europol. Prominent features in this regard are independent data protection supervision, Europol's secure information exchange capabilities, data protection compliant outreach to the private sector and – most importantly – clearly defined purpose specifications for processing operations upon personal data in Europol's databases.

The aims of preventing and combating cybercrime are balanced against the goal of safeguarding the freedom of individuals. In fact, they go hand in hand: at Europol, it is recognised that the data protection rules in place are essential for the success of operations. High data protection standards lead to high quality of data which itself is a precondition for high quality crime analysis.

3.3 What is Forensic Computing?

Felix C. Freiling (Friedrich-Alexander-Universität Erlangen-Nürnberg, DE)

We discuss the different notions of digital forensics, computer forensics and forensic computing in context and try to approach a useful meaning of the term "forensic computing". We argue that any notion of forensic computing should be defined in comparison to fundamental theories in traditional forensic science. We propose a separation of what is currently demanded of practitioners in digital forensics into a rigorous scientific part on the one hand, and a more general methodology of searching and seizing digital evidence and conducting digital investigations on the other. We thereby mark out the route for computer forensics to turn into a true forensic science.

3.4 Internal Investigations, IT Forensics and Law

Dennis Heinson (Hamburg, DE)

Internal investigations in enterprises are, alongside criminal investigations conducted by state authorities, the main field in which IT forensics get performed. The legal regime that governs such investigations is substantially different to the law of criminal procedure which applies to criminal prosecution. While issues such as admissibility and relevance of evidence are largely in accord between both procedural regimes, the rules that govern the collection of evidence differ fundamentally.

For in internal investigations the private entities that collect evidence are not bound by the strict rules of the code of criminal procedure. Instead, mainly data protection laws may constrain the permissible means, scope and depth of an examination. In it, as a general principle, an investigation must be justifiable both with regards to the suspect as well as any third persons whose data gets processed during the course of the investigation. The applicable provisions contain no clear-cut criteria as to the "if's" and "how's" of an investigation, but instead mark the outer boundaries of what is allowed. Generally, only suspicion based on facts that an employee has commited a crime may trigger an investigation.

3.5 Fingerprinting Techniques for Network Forensics

Dominik Herrmann (Universität Hamburg, DE)

Joint work of Herrmann, Dominik; Fuchs, Karl-Peter; Federrath, Hannes
Main reference D. Herrmann, K.-P. Fuchs, H. Federrath, "Fingerprinting Techniques for Target-oriented Investigations in Network Forensics," to appear in Proc. of GI SICHERHEIT 2014, März 2014.

Fingerprinting techniques are receiving widespread attention in the field of information security. This talk shows why they may be of specific interest for the field of network forensics. Firstly, fingerprinting techniques can be used to infer the activities of suspects, even when communication is encrypted. Secondly, they can be used to associate criminal activity with a suspect, even in the absence of explicit identifiers. In order to illustrate the utility of fingerprinting techniques three case studies are introduced. For each case study the applicability of existing as well as new fingerprinting techniques, which are based on DNS queries, is reviewed. Finally, some arguments are provided in order to start a discussion about the opportunities and risks that may result from using evidence gained by fingerprinting techniques in criminal investigations.

3.6 The fundamental rights dimension of individual and mass surveillance

Gerrit Hornung (Universität Passau, DE)

Forensic computing regularly interferes with fundamental rights, such as informational self-determination, confidentiality and integrity of IT systems, fair trial etc. These rights form different layers with different supervisory bodies, leading to complex material and procedural situations. This becomes even more complex when compared to the US situation, when the FISA court recently denied that so-called meta data enjoys the protection of the fourth amendment. We discussed the limitations of judicial review in the area of secret agency surveillance post-Snowden, as well as possible topics to discuss in the seminar deriving from the fundamental rights dimension.

3.7 Forensically Sound Data for Digitised Forensics on the Example of Locksmith Forensics

Stefan Kiltz (Universität Magdeburg, DE)

Joint work of Stefan Kiltz, Eric Clausing, Jana Dittmann, Claus Vielhauer

In a lot of disciplines in crime scene forensics (e.g. ballistics, dactyloscopy, forensic locksmithing), research is conducted to introduce IT systems to support the forensic experts off strenuous, repetitive and error-prone task (termed as digitised forensics). Instead of analysing physical objects, digital representations of some aspects of the physical world are investigated after an analogue to digital conversion. Often this involves pattern recognition as a means to basically enhance the contrast between a latent trace and the surrounding environment, which could employ machine learning and statistics based approaches.

Digitised forensics both brings new opportunities (e.g. when using contactless sensory little or no influence of the investigation process on the recovered artefacts) but also brings on new challenges (e.g. if latent traces are rendered visible only in the digital domain, how can the process still be comprehensible also for technical laymen such as the judge). As a direct consequence of the latter, two chains of custody need to be maintained, the conventional chain of custody for physical objects but also a new chain of custody for digital objects. As with the conventional, also the chain of custody for digital objects needs to adhere at least to the security aspects of integrity and authenticity.

To model the process (a model as a means to ensure comprehensibility), existing models for the forensic process for IT forensics can be successfully adopted. It has been researched, that the splitting into several investigation steps and their order of execution is vital to achieve comprehensibility and thus transparency by allowing to annotate the different forensic data types with the investigation process of the input data and with the investigation process of the output data. This allows to identify dependencies, which can be vital e.g. if some piece of data is identified to be bad or erroneous late in the investigation process. In such cases all other data and the conclusions drawn from its interpretation needs to be identified and marked as also inaccurate and, if possible, re-investigated.

This talk is based on the following two articles:

- Stefan Kiltz, Jana Dittmann, Claus Vielhauer: “Beweissichere Daten in der digitalisierten Forensik”, In D-A-CH Security 2012: Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven. Konstanz, Germany. 25.–26.09.2012, IT Verlag Sauerlach, ISBN 978-3-00-039221-4, pp. 288–300, 2012.
- Stefan Kiltz, Eric Clausing, Jana Dittmann, Claus Vielhauer: “Ein Vorgehensmodell für die digitale Schlossforensik”, In D-A-CH Security 2013: Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven. Nürnberg, Germany, 17–18.09.2013, syssec, pp. 367-379, ISBN 978-3-00-042097-9, 2013.

3.8 Experiences from drafting the cybersecurity act in CZ

Radim Polcák (Masaryk University, CZ)

When cybersecurity becomes a legislative issue, there is a need to tackle it not primarily as technical but rather a social phenomenon. In that sense, the duties laid down by qualitatively new sort of legislative provisions have to be grounded on proper material legitimacy. In particular, there is no such thing as “security,” whereas there is always a need to ask as to “what” is to be secured. In the case of cybersecurity, the primary concern is to create an environment for individuals to exercise their fundamental information rights, most of all the right for information self-determination (this complex concept includes passive protective rights towards privacy and personal data as well as active rights to have an opportunity to use services of information society in order to engage in social interaction) and freedom of speech.

In the Czech Republic, as well as in the case of other post-communist countries, there had to be especially tackled issues related to content-oriented regulation and institutional backing. Experience with communist censorship as well as with the situation in which the state is understood as an enemy of a person, enhances social and political sensitivity of the regulatory task. Consequently, the Bill, apart from being based on the idea of protection of individual information rights, was built upon the principle of technology neutrality as well as on institutional distinction between security and law enforcement. Consequently, the agenda was entrusted into the hands of the National Security Authority, whereas possible use of information gathered in the course of security operations are to be made available to other branches of state executive upon standard principles of transparent inter-institutional cooperation.

The paper, apart from explaining the aforementioned fundamental regulatory concerns, discussed also particular regulatory features of the legislative draft – namely the system of reporting and processing of data on security incidents, cooperation between national and governmental response teams as well as possible consequences of drafted EU common regulatory framework.

3.9 Basics zum Beweisrecht im Strafverfahren

Tobias Singelnstein (Freie Universität Berlin, DE)

Das Strafverfahren gliedert sich in drei aufeinanderfolgende Phasen. Es beginnt mit dem in der Praxis äußerst wichtigen Ermittlungsverfahren, das von der Staatsanwaltschaft geleitet wird. Hieran schließen sich das Zwischen- sowie dann das Hauptverfahren an, wo die Verfahrensherrschaft beim Gericht liegt. Für den Beginn eines Ermittlungsverfahrens ist ein Anfangsverdacht erforderlich, d.h. konkrete tatsächliche Anhaltspunkte, dass eine Straftat begangen worden ist. Will die Staatsanwaltschaft am Ende des Ermittlungsverfahrens Anklage erheben, so benötigte sie hierfür einen hinreichenden Tatverdacht, also die Wahrscheinlichkeit einer Verurteilung im Hauptverfahren. Das Gericht schließlich benötigt für sein Urteil am Ende des Hauptverfahrens die richterliche Überzeugung von der Schuld des Angeklagten. All dies – Anfangsverdacht, hinreichender Tatverdacht, richterliche Überzeugung – wird aufgrund von Beweismitteln beurteilt, die vor allem im Rahmen des Ermittlungsverfahrens gesammelt werden.

Dabei sind die Strafverfolgungsbehörden einerseits verpflichtet, den Sachverhalt bestmöglich aufzuklären. Andererseits unterliegen sie rechtlichen Grenzen. Ermittlungsmaßnahmen zur Beschaffung von Beweismitteln stellen in aller Regel Grundrechtseingriffe dar. Solche Eingriffe sind nur aufgrund einer hinreichend bestimmten gesetzlichen Grundlage zulässig. Fehlt es an einer gesetzlichen Grundlage oder sind die Grenzen dieser Grundlage im konkreten Fall überschritten worden, so ist die Beweiserhebung rechtswidrig und die erlangten Beweise dürfen unter Umständen im Prozess nicht verwendet werden. Dies ist der Fall wenn ein so genanntes Verwertungsverbot vorliegt.

3.10 Surveillance of US-surveillance

Erich Schweighofer (Universität Wien, AT)

This talk presented a discussion outline of a legal assessment of US-surveillance in Austria.

4 Discussion Groups

4.1 Digital Evidence

Dominik Herrmann

The discussion group on the topic of "Digital Evidence" consisted of participants with a background in law as well as participants with a background in information security and digital forensics.

The group looked at particular issues related with the collection and interpretation of digital evidence during criminal investigations. The discussion started out with four main questions: What sorts of evidence can be collected? Is the collected evidence good enough to substantiate specific claims? How can digital evidence be collected, i. e., what are the requirements for evidence collection procedures? What types of digital evidence are law enforcement agencies allowed to collect?

Participants felt that especially the "problem of probabilities", i. e., high accuracy values given for newly proposed forensic techniques in scientific papers are an issue. High accuracy values convey a false sense of confidence, although the techniques have never been put to the test in a practical environment. As a means to address this issue, participants suggested to work on the standardization of collection and analysis procedures in practical settings.

The discussion raised two questions: Firstly, there was a debate whether digital evidence can be fabricated or faked more easily due to the fact that information does not degrade when it is copied. On the other hand, it may be more difficult to commit a crime in a digital environment without leaving behind any traces at all. Secondly, there was no agreement on the question whether digital evidence may lead to unfair court trials. Some participants reported that the defense lawyers may find it difficult to question the validity of digital evidence, when the prosecutor is not willing to hand over the raw data..

All in all, due to its interdisciplinary composition, the discussion group provided an environment for a fruitful exchange of technical as well as legal aspects.

4.2 Cross-border cloud investigations

York Yannikos

The topic of this discussion was identifying problems and potential solutions regarding digital forensic investigations in cloud environments. Since the technology used in cloud computing poses new questions for experts in digital forensics and law, several aspects were discussed from a legal and a technical point of view.

The following topical question fields were discussed:

1. What are the currently used methods to acquire digital evidence stored in the cloud? What are the legal requirements?
2. Is it possible to locate evidence data stored in the cloud in a reliable way? What could be done if evidence data could not be located (i.e., the country/countries are unknown where the servers are located on which the data is stored)?

3. What methods/technology could be used in the future to allow a lawful interception of cloud environments?
4. Is it legal to access potential evidence data stored in the cloud through the data owner's computer, e.g., during a house search?

The following sections summarize the results taken from the discussion.

Acquisition of digital evidence in the cloud

By now, cloud data is typically acquired by first localizing where the data is stored in order to go there and seize the corresponding storage hardware or clone any relevant virtual machines. After that, a forensic analysis of the seized storage/VMs is performed. Obviously, without a successful localization of the data and the corresponding hardware the data has to be acquired in a different way.

Currently, existing laws typically regulate access to physical assets or devices where assets are stored. No laws exists which deal with cloud data acquisition in forensic investigations; the consensus of the discussion group was however that such laws are urgently needed.

Localization of digital evidence in the cloud

Currently no standardized techniques/approaches are available for forensic investigators which would allow a reliable data localization in the cloud. Cloud storage technology makes it not only difficult to identify and locate the hardware where specific data stored, but even the countries where the hardware is located could be hard to tell.

One approach to access cloud data that could not be localized is by using credentials provided by the cloud service provider (CSP). However, this requires the CSP to cooperate and becomes a difficult and/or very time-consuming task e.g., if the CSP is based in another country with different legislation.

Another approach is wiretapping the communication between user and CSP. However, this could require data decryption or reverse engineering of the used protocol which drastically increases the difficulty to access the data.

Future evidence acquisition in the cloud

Theoretically, specific APIs allowing a lawful interception of cloud data could be implemented by the CSPs, but in practice such APIs currently do not exist. However, it is very likely that some kind of forensic API will be provided by the CSPs in the future, but corresponding legal regulations have yet to be defined.

When forensic APIs are available at some point in the future, it is very important to implement controls which strictly regulate and document any use of the APIs in order to prevent abuse and ensure that they are used only for lawful interception.

Legal issues of evidence acquisition in the cloud

Two different opinions were stated within the discussion group:

From the legal point of view, there is no specific law regulating data access in cloud environments. Therefore, existing laws which currently regulate access to assets residing in specific countries have to be applied. As a consequence, access to data in cloud environments is legally permitted only if the location of the data is known and if a legal agreement which permits access to the data exists with the country where the data is localized. This holds also for data which could be possible evidence.

However, from a technical point of view, accessing data stored in the cloud by using the data owner's computer should be allowed, e.g. when the data owner is currently logged into his cloud storage account. Technically, it makes not much sense to restrict access to data stored in the cloud just because the storage location of the cloud data is not known, since the data itself is typically accessed/processed at the data owner's computer, much like the data stored on the local hard drive.

4.3 Forensics vs. Privacy

Felix Freiling (Friedrich-Alexander-Universität Erlangen-Nürnberg, DE)

Joint work of Gerrit Hornung, Nicolas von zur Mühlen, Dennis Heinson, Jan Ellermann, Hannes Federrath, Andreas Dewald

The discussion group quickly realized that the proper title of this group should have been "Forensics and Data Protection". This is more general and points to many critical aspects of digital investigations of which the community is largely unware. This is slowly changing, as indicated by Jan Ellerman, who stated that at Europol, forensic workplaces are filmed and the filmed material is later reviewed to check for proper evidence handling.

Data protection concerns both the collection of evidence and the use of evidence in court. The main legal restriction, at least in Germany, is the *protection of the core area* ("Kernbereichsschutz"). It is constitutionally required to protect the core area of privacy in all procedures. For example, in so-called online searches (collection of evidence through a trojan on the computer of a suspect) a data protection officer, a lawyer and one other person must check and possibly delete data which is considered to belong to the core area.

In digital forensics, the principle of data avoidance is important not only because of the huge amount of data collected by law enforcement. But data avoidance is in conflict with data retention. It was discussed, whether this is part of forensic computing? Another issue of data protection is the sharing of data across borders, e.g. with states that are assumed not to respect human rights in a way that we would expect.

The group did not finish to discuss all relevant problems. More specific questions were to be discussed if group continues (which it unfortunately did not). As a bottom line, all participants agreed that it is important to raise data protection awareness in digital investigations.

4.4 Offensive Countermeasures

Thomas Schreck (SIEMENS CERT München, DE), Michael Gruhn (Friedrich-Alexander-Universität Erlangen-Nürnberg, DE)

Joint work of Felix Freiling, Thomas Schreck, Radim Polcak, Vaclav Stupka, Michael Gruhn, Tatiana Tropina

The discussion was based on five scenarios:

1. Hacking into systems to identify the attacker

Attackers are using several techniques to hide their identification. One way is to hide themselves behind proxy chains provided by different hosting providers or compromised computer systems and located in different countries. In order to identify the attacker, an investigator must follow the chain of proxies back. One way is to break into each system until the attacker's system is identified. There the analyst is able to collect information about the attack and person. A different, often unpractical way, for an investigator is to subpoena her way through the proxy chain. However, because of different jurisdictions this is tedious, sometimes even impossible, and most of the time takes too long to catch an attacker red handed or even at all.

2. Stealing back data an attacker gathered, e.g. via a trojan

Criminals are using so-called dropzone systems to collect stolen information, such as user credentials, online banking credentials, and documents. These dropzones can be readily identified by analyzing the malicious software. However in order to "get the data back", i.e., determine what data has been compromised and act accordingly, it is often necessary to exploit vulnerabilities within the dropzone software to get access to the system. However, again the legal basis for this is unclear, because especially private investigators would be using unauthorized access in violation of some law. Further again the problem of jurisdiction makes this approach difficult to judge legally.

3. Sinkholing malicious systems

IT security researchers are using a technique called "sinkholing" to redirect malicious traffic originally sent to a so-called command and control (C&C) server, to a sinkhole, i.e. a system that analyzes and rejects bad traffic. However, legally this could, in some jurisdictions, be violating telecommunication laws, because the original traffic is diverted, i.e., intercepted.

4. DoS against attacker's controlled systems

The most common attack type on the Internet are denial of service (DoS) attacks. In a DoS attack a malicious entity overloads the service provider with bogus request so legitimate users are denied access to the service. A very simple idea to interrupt the operations of attackers is to use a DoS attack against them. However, there is no explicit legal basis for self-defense on the Internet, hence, such actions, especially when interrupting the service of infrastructure not belonging to the attacker, e.g., intermediate routing networks between the attacker and the investigator, can make these actions just as illegal as the operations of the attacker.

5. Blacklisting and blocking of malicious systems

Another simple way to stop malicious operations is to blacklist and block the systems used to facilitate them. An example for this are the various blacklists for web servers sending spam emails. However, sometimes spammers use legitimate mail servers or networks of hosting providers for their activities. It thus often happens that the mail or hosting providers IP range is blacklisted, even though the mail or hosting provider has already removed the malicious user from their service. This can lead to DoS against the mail or hosting provider. Legally there are no clear guidelines to whether or not a service provider, here the mail providers receiving mail from a blacklisted system, has the right to freely choose whom he provides service to or not. However, this clearly violates net neutrality.

The conclusion of the discussion was that many of the new and often offensive methods that investigators can deploy are not very well covered by the current laws, and depending on how the laws are interpreted and what jurisdictions are competent some of these actions may or may not be legal. However, clear consensus could not be reached. Practical forensic investigators voiced their pledge for clearer laws on the matter.

4.5 Internal investigations

Christian Hawellek (Leibniz Universität Hannover, DE), Michael Gruhn (Friedrich-Alexander-Universität Erlangen-Nürnberg, DE)

Joint work of Gerrit Horrnung, Christian Hawellek, Dennis Heinson, Thomas Schreck, Radim Polcak, Andreas Dewald, Sven Kälber, Michael Gruhn
Main reference Article 82 of the proposed EU General Data Protection Regulation

In this discussion group Article 82 of the proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) was discussed.

First the article was read by everyone and immediately the paragraph 1 c) was found to be of particular importance, as it proposes that "processing of accumulated traffic data shall be permitted in particular to ensure data security", however, the term "data security" is not defined in the terms of Article 82. Instead Article 30 regulates data security, its scope and protection of personal data. However, by going through these definitions the definition of profiling was confusing and found to be impractical, because searching log files for heuristics, such as attack signatures, needs to be done without existing suspicion, but this would be inadmissible profiling according to the proposed regulations.

It was discussed whether this searching for heuristics is really profiling. The proposal defines profiling in Art. 4 Par. 3 a). It states that "'profiling' means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour". By this definition technical profiling even without personal profiling is hardly possible, as is any form of data aggregation.

Thus it was discussed whether Art. 82 Par. 1 c) is lex specialis against Par. 1 a) and whether technical detection was sufficiently considered in the proposal. One possible argument that makes profiling legal under Art. 4 is when the intentional element is missing, i.e., the data is not intentionally aggregated to gain personal information, but to investigate attacks. For example, an investigator collects all emails, data on a system and browser history, then performs a key word search on this data. In this circumstance it would be a compliance investigation search and Par. 1 c) would apply.

Discussing the impact of these definitions it was agreed that the definition of profiling is too broad. Depending on how the definition is interpreted it may apply to all investigations of IT security teams, as they are always automatically process data involving certain personal aspects. However, reading the definition thus that a personal profile needs to be the result of profiling may exclude those cases in which only a technical analysis takes place for IT security reasons.

Because of time constraints further definitions, e.g., for “freely given consent” were not discussed.

However, the question whether profiling actually exists in companies was briefly discussed. One such example is Google. Some years ago they tried to predict how likely an employee would be to quit from their web browsing habits to be able to react on this proactively. Pseudonymization might be a way to avoid the risk of such profiling being applied, however, pseudonymization is not possible with unstructured data.

The next issue that was discussed was the term “appropriate” in Par. 1 c). Par. 1 c) deals with deadlines for deletion of gathered data. There used to be an allowance for judgment depending on the circumstances of the case. However, in the proposal it is unclear whether deadlines for deletion refer to the individual investigations or not. This is problematic because the provision refers to “processing” and to “investigating” both the same. It is also unclear whether or not a general information such as “your email traffic will be under surveillance” is sufficient for compliance, because this would create some sort of general knowledge.

The proposal further does not cover routine checks, e.g. checking employees computers for malware such as trojans. A particular suspicion is always required if personal data is concerned. A highly problematic scenario is that general surveillance may exists in a company, from which suspicion is raise about a particular incidence, on the basis of which an investigation is initiated. However, it could also be that such information is used to retroactively justify the investigation by not revealing that only due to the surveillance measure the suspicion has been created in the first place. Another concern is proportionality as it applies to both the process of collection as such and the nature and extent of the data collection it remains unclear whether “data collection” in the second half of the Par. 1 c) refers to the process or the outcome. It is also unclear what “nature of data collection” means. Is the purpose the nature or is the way in which the data is collected the nature?

Par. 1 c) (a) further states “the investigation shall be carried out by the competent authority” but it is undefined whether “investigation” and “authority” refer to public authorities’ investigation or private investigations. Whereas the terms very much indicate so, it would be difficult to put this in context with the alternative of “serious dereliction of duty in the employment” context.

Par. 1 d) again raised terminology discussions between forensic practitioners and the legal professionals. The questions discussed were: What does data security mean? What is accumulated traffic data? Does it mean anonymous? Why are “Internet” and “email” mentioned separately? To include email in private networks? Is traffic data the same as content data? Technically the paragraph states that only meta data shall be analyzed. But this is not effective for data security. Cannot not be used for preventive measures (Lacuna).

Besides the main topic also the wording of laws in general was discussed spearheaded by the question why is the word “must” sometimes changed into “shall”? This could have historic reasons and possibly to emphasize the normative element. But does not change the meaning because “shall” can be replaced with “must” without changing the meaning of the law text.

To summarize, the following problems have been carved out during the discussions that are not very well covered by the proposed regulation:

- content data (what is it and is it personal or not?)
- preventive measures (monitoring for threat detection)
- wording (internet, data security, profiling)
- external attackers (lacuna)
- server forensics (exemption missing for fragments of personal data).

Participants

- Andreas Dewald
Univ. Erlangen-Nürnberg, DE
- Jan Ellermann
Europol, NL
- Hannes Federrath
Universität Hamburg, DE
- Felix C. Freiling
Univ. Erlangen-Nürnberg, DE
- Michael Gruhn
Univ. Erlangen-Nürnberg, DE
- Christian Hawellek
Leibniz Univ. Hannover, DE
- Dennis Heinson
Hamburg, DE
- Dominik Herrmann
Universität Hamburg, DE
- Gerrit Hornung
Universität Passau, DE
- Sven Kälber
Univ. Erlangen-Nürnberg, DE
- Stefan Kiltz
Universität Magdeburg, DE
- Volker Krummel
Wincor-Nixdorf International GmbH – Paderborn, DE
- Radim Polcák
Masaryk University, CZ
- Thomas Schreck
Siemens – München, DE
- Erich Schweighofer
Universität Wien, AT
- Tobias Singelnstein
Freie Universität Berlin, DE
- Vaclav Stupka
Masaryk University – Brno, CZ
- Tatiana Tropina
MPI für Strafrecht – Freiburg, DE
- Nicolas von zur Mühlen
MPI für Strafrecht – Freiburg, DE
- York Yannikos
Fraunhofer SIT – Darmstadt, DE
- Riha Zdenek
Masaryk University – Brno, CZ