Court Rulings as Evidence for Social Engineering Research

Bachelor Thesis

Ngoc-Minh Michal Pham

November 9, 2015

Supervisors:

Prof. Dr. Dieter Gollmann

Dipl.-Math. oec. Sven Übelacker

Hamburg University of Technology

Security in Distributed Applications

`https://www.sva.tuhh.de/`

Am Schwarzenberg-Campus 3

21073 Hamburg

Germany

Thanks to Sven Übelacker for dedicating his time supporting me throughout the thesis.

Declaration

I, Ngoc-Minh Michal Pham, solemnly declare that I have written this bachelor thesis independently, and that I have not made use of any aid other than those acknowledged in this bachelor thesis. Neither this bachelor thesis, nor any other similar work, has been previously submitted to any examination board.

Hamburg, November 9, 2015

Ngoc-Minh Michal Pham

Abstract

English: Many researchers conduct Social Engineering (SE) research on the basis of Kevin Mitnick's collection of SE attacks, though these attacks are missing evidence. This Thesis discusses the viability of court documents as research material for SE as an accurate source of information. Several court documents were retrieved from a public database using the keyword "Phishing" and the law for computer-fraud. They were sorted into a subset of documents containing SE using Mouton's definition of SE and categorised using principles by Cialdini/Stajano and finally analysed for descriptions of SE attacks. Challenges encountered during the process were non-uniform record keeping and the lack of focus on exact process documentation. In conclusion it was determined that court documents have definitely a statistical use. Whether they can be used for precise SE attack analysis can only be seen on a case by case basis. Nevertheless, the set of analysable documents can be expanded by using different search criteria on subsequent searches and different sources.

Deutsch: Viele Wissenschaftler basieren ihre Forschung in Social Engineering (SE) auf der Basis von Kevin Mitnicks Sammlung von SE-Angriffen, auch wenn diese größtenteils ohne Beweislegung dargestellt werden. Die Thesis befasst sich mit der Nutzbarkeit von Gerichtsurteilen als Forschungsmaterial für genaue Informationen über SE Angriffen. Gerichtsurteile wurde von einer öffentlichen Datenbank mit dem Stichwort "Phishing" und dem Gesetz für Computerbetrug §263a StGB genommen. Diese wurden in eine Untermenge von Urteilen mit SE sortiert mit der Benutzung von Moutons Definition von SE, kategorisiert mit Hilfe von Prinzipien von Cialdini/Stajano und letztendlich analysiert nach Beschreibungen von SE-Angriffen. Herausforderungen waren unter Anderem die nicht uniforme Aufnahme von Informationen in den Gerichtsurteilen sowie das Fehlen der exakten Prozessdokumentation. Die Schlussfolgerung war, dass Gerichtsurteile zumindest einen statistischen Nutzen haben. Ob dies auch für präzise SE-Angriffsanalyse genügt, kann man nur von Fall zu Fall beurteilen. Trotzdem kann die Menge der zu analysierenden Gerichtsurteilen mit anderen Suchkriterien und Quellen erweitert werden.

Contents

1. Introduction

In today's world, humans attend to daily business using technology to communicate with each other and other activities. While the design behind the technology is equipped with security measures to prevent undesired events, the human often proves to be the deciding factor when it comes to effective security. Be it against a single person or an entire organisation, a well prepared so called Social Engineering (SE) attack can easily penetrate the security set up by the targets. SE today is an active research field with many research topics already established, like frameworks to better understand single components of SE attacks and methodologies to select effective countermeasures against them.

A common theme among them is that they are based on Kevin Mitnick's collection of SE attacks contained in his book "The Art of Deception" [1]. That is fine as long as the attacks are not taken as the absolute truth. They are useful in the sense that they are plausible in reality, however being plausible is also the best they can offer. Mitnick has a history of crimes involving computers and/or communication and can speak out of his own experience. The problem is, that most of his stories or experiments are not backed up by evidence and have the ever so slightly chance of being completely fabricated. Therefore, if someone requires a set of real world data of SE attacks, they will not find the reality in Mitnick's collection, as the guarantee for accuracy is missing. Basing research on unconfirmed data might not be the best idea in a scientific field, as a lack of citations will severely reduce the credibility of the data source and the research itself

So this bears the question: where can we obtain reliable information about real SE attacks?

1.1. Document Structure

In Chapter 2 I will first go into the process of how I came to the decision of taking court documents into consideration as a source of information. Chapter 3 will provide a list of definitions and terms used in the remainder of the thesis. Following that comes the methodology in Chapter 4 to give an idea about how I proceeded with the analysis, as well as a few examples. As additional information, Chapter 5 gives a breakdown of German court rulings to show what a document consists of. I will then go into the results of the analysis in Chapter 6 and follow up with the conclusion in Chapter 7.

2. Gathering Information on Social Engineering

At the time of writing there are not any notable organisations that specialise in documenting SE cases. Though there are some to be considered that may include SE in their broader expertise. Considering the nature of SE attacks, it is clear that the victim are most likely the first person witnessing the techniques employed against them.

A source of information that includes a person who was in direct contact with the victim could be publicly available news articles that report on topics like “deception” and “fraud”. This does not seem far off the mark considering that the research by Stajano et al. started off as a TV show [2]. But the lack of integrity in how facts are being reported poses a problem when scientific research is supposed to be based on it. News articles may be perceived by someone as a medium to report the truth unadulterated, but when it comes to the financial purpose, many of them have a steady readership to keep in tow. There is always the possibility of an editor putting their own spin on the events to make an article more interesting. On top of that the details of a SE attack is not a very appealing topic in the average human life. At least not appealing enough to commonly find articles about them in the daily newspaper or the front-page of established news outlet websites. In addition, journalists themselves do not always have enough time and background to research the facts properly. With that said, it is not impossible to encounter written explanations of SE attacks in a news article on the internet, just not enough to base a detailed analysis on.

Another alternative could have been a police database containing the details of filed complaints and crime reports, assuming that SE victims report to the police. However, access to a database of a state entity is usually restricted to the public and attempts to ask for permission from authorised police officers proved fruitless. That does not mean that all information gathered by the police ends up being locked away. The Police Crime Statistics released by the Federal Criminal Police Office every year (also in English) gives insight into the numbers that are officially recorded [3]. These numbers are reported to police directly from the so called “dark field”, leaving anything behind that does not come to the police’s notice. When thinking further about where the reported information ends up, it comes to mind that court trials may be initiated if the aggressor is present or under special circumstances. If a court comes to a decision regarding a case, that decision, along with the entire process, is documented. And that leads me to the next possible source of information: court documents.

2.1. The Search Process

There is no doubt that a court will strive to be as accurate as possible when determining the facts of the events of a crime. Therefore I can at least continue with the promise of guaranteed effort put into the quality of the sources of information. It differs from state to state, but court documents are publicly available, if at a price. For this thesis the database provided by Juris GmbH was used. As for what was searched for, Prof. Hoeren wrote a good documentation about relevant laws used in Germany regarding internet law [4]. Specifically for this thesis I decided to limit the analysis to something distinctly recognisable, namely phishing. According to Prof. Hoeren, possible laws that can be applied include:

- Possible law for phishing in general is § 263 Strafgesetzbuch (penal code) (StGB), which covers fraud
  - Phishing for information is seen as preparation for computer-fraud, described in § 263a(3) StGB, which specifically goes into "the creation, acquisition, providing or storing" of computer programs designed to perform computer-fraud
- Data espionage (i.e. account credentials) falls under § 202a StGB
- Falsification of evidentiary data covered by § 269 StGB
- Data manipulation and computer-sabotage through §§ 303a(1), 303b(1) Nr.1 StGB when applicable

Included but for this purpose less relevant are the following laws:

- §§ 143, 143a Markengesetz (law for brand protection) (MarkenG)
- §§ 106 and continuing Urheberrechtsgesetz (copyright law) (UrhG)

2.2. Court Documents as a Source of Information

To summarise: Phishing in Germany encompasses a series of actions on which a set of laws can be uniformly used against. The law I believe to be the broadest container of SE is §263a of the StGB, computer-fraud. At first I tried many different related laws as search criteria, however there were not enough results or too many unrelated entries for each of them. Finally, using the computer-fraud law as a paragraph and "Phishing" as a keyword, the database returned the desired quantity of documents to work with. If court documents can provide detailed descriptions of SE attacks, it is possible to re-conduct and re-evaluate these attacks for further research. However, companies that publish court documents usually have set of general terms and conditions that restrict the publication their content by third parties. This can have problematic consequences when releasing papers with parts of their documents. I ultimately refrained from including a page from a court ruling exactly because of this reason. If in doubt, do not include any licensed content and ask the provider for information.

2.3. About Juris GmbH

Court rulings in Germany are not (yet) made freely available automatically, requiring companies such as Juris GmbH to publish them. Juris GmbH is a publishing company with focus on legal documents and information. They prepare and provide a wide variety of document types including court rulings, magazines, law definitions, comments and more through their website online. Their database can be searched through without a membership, but only abstracts can be read while doing so. Usually a fee has to be paid to utilise some of their services, but in the case of this thesis the database was accessed through the library in the university of Hamburg. Juris GmbH has partnerships with different universities to provide students and other academically interested people free access to their services.

3. Definitions

Several definitions were used as a basis for the analysis. They served as guidelines for identifying SE or assigning them with recognisable key attributes. Doing so reduced the workload of managing and analysing the documents.

3.1. Social Engineering by Mouton

Mouton has extensively occupied himself with the definition of SE and how to properly streamline the understanding of it [5]. I supported my analysis with the following definition from his work:

> "The science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity".

A simple occurrence of SE is gaining unauthorised access to a company building by carrying a large stack of boxes and asking a person who is exiting to hold the door open. Out of kindness they will comply with the request. A more common example are phishing mails trying to trick the recipient into clicking a link and disclosing their sensitive information. These occurrences are called SE attacks and incorporate so called social principles.

3.2. Principles of Persuasion by Cialdini

One thing to note is that Cialdini defined his principles while working in the marketing department, meaning that his principles were not originally designed to portrait illegal or hostile exploitation. He focuses on the target as the acting entity and his principles represent different exploitable social constructs of today's society. They answer the question of why the target is acting. The following descriptions were not directly taken out of Cialdini's definitions, but rather from Bullée's work.[6]

> **Reciprocity:** "Refers to the giving of something in return. The target feels indebted to the requester for making a gesture. Even the smallest gift puts the requester in an advantageous position."

It does not have to be the conventional giving of something of value like money or being the first one to give. As long as the target sees value in it, you can gain an advantage in giving it (or pretending to do so). Many marketing campaigns for example promise rewards for a few lucky chosen for spreading

the word of their brand on Facebook. A SE attack using reciprocity could involve requesting bank information in order to pay back as "compensation" for something.

Conformity/Social Proof: "Is imitating the behaviour of other people. Members of the in-group have a stronger feeling of group-safety compared with members of the out-group."

Utilising social proof is, in other words, based on convincing or proving to the target that something is (socially) acceptable. One example of this are bartenders who fill their tip jar beforehand to make patrons believe the presence of generosity from other people. The principle may remind you of the phrase "All the cool kids are doing it!". In a more sinister sense, social proof can be used by attackers to steer the target into any desired action through convincing argumentation.

Liking: "Liking someone puts that person in a favourable position. People tend to like others who are similar in terms of interests, attitudes and beliefs."

An evident example are celebrity associations with advertised products, which fans want to follow suit. However there are many reasons why someone may like another person, though it does not even have to be a person. Pleasing visuals of websites and other inanimate objects can equally make the target feel comfortable about doing desired actions as an example.

Scarcity: "Occurs when a product, service, or information has limited availability. People therefore perceive an increased value and attractiveness towards these products, which makes them more desired than others."

Making someone feel like that something they value is going to be out of stock very soon is a very common sales tactics. In SE the attacker can simulate the scarcity of value in order to manipulate the target into accepting certain actions like revealing information or sending payment.

Commitment: "Refers to the likelihood of sticking to a cause or idea after making a promise or agreement. In general, when a promise is made, people will honour it, which increases the likelihood of compliance."

Commitment is also present as a simple desire to be consistent. An example would be auction sites where there is a strong desire to place a higher bid after being outbid by someone else after having initially placed a bid already. In SE this principle is commonly seen as a contract for a job that initially looks legit. Being bound to something by documents that are legal in appearance will likely make them stick to whatever an attacker has planned out for them.

Authority: "Is the principle that describes people's tendency to obey the request of authoritative figures. If people are unable to make a well-informed decision, the responsibility to do so is transferred to the group or person they believe is in charge. Crisis and stress activate the behavioural trait of responsibility transition."

Bullée elaborated further on the authority principle with multiple types of authority based on hierarchy, appearance and others. Authority by hierarchy is something commonly seen in corporate structures. Employees with higher ranks have increased access and freedom within a company than others. Authority by appearance is as simple as it sounds. An experiment showed that more people tend to follow a person in a suit through a red traffic light than someone in casual clothes simply because they think the person in the suit emits authority. Even though this example was used to explain the authority principle, it is also related to the conformity principle. Instead of following because the crossing person can just do it, one might think that it is socially acceptable to cross the red traffic light.

3.3. Principles Identified by Stajano

Stajano's principles originated from an educational TV show that taught viewers about common scams and how to avoid them. The principles are designed around the attacker being the acting entity and the principles encompass different attributes in addition to social constructs. Stajano explained in great detail how each principle is used to manipulate the target.

Distraction: "While we are distracted by what grabs our interest, hustlers can do anything to us and we will not notice."

Something that "grabs our interest" can also be a thing of everyday life: something we have to do that we are used to, but do not particularly have any interest in. Be it everyday necessities like house chores or more relevant to this cause, recurring message prompts on computers and other devices. Being so used to these activities makes us quite prone to distraction or saving time while doing them.

Social Compliance: "Society trains people to not question authority. Hustlers exploit this 'suspension of suspiciousness' to make us do what they want."

This principle correlates strongly with Cialdini's authority principle so there is no need to explain any further.

Herd: "Even suspicious marks let their guard down when everyone around them appears to share the same risks. Safety in numbers? Not if they are all conspiring against us."

This principle is the equivalent of Cialdini's social proof principle, with the difference that Stajano explains the "herd" to be also part of the attacker group. It still comes to the result that the target believes an action to be an acceptable choice if other people are appearing to be doing the same.

Dishonesty: "Our own inner larceny is what hooks us initially. Thereafter, anything illegal we do will be used against us by fraudsters."

This principle could be responsible for why many illegal activities are not reported to the police or other authorities. Convincing a target to initially comply with something (not obviously) illegal makes it a lot harder to report it later to authorities because the target is also part of it.

Kindness: "People are fundamentally nice and willing to help. Hustlers shamelessly take advantage of it."

An example was given in Section 3.1, but kindness can be exploited in many different and unpredictable ways.

Need and Greed: "Our needs and desires make us vulnerable. Once hustlers know what we want, they can easily manipulate us."

In this case desire is a principle in itself, making targets comply with demands simply because they want something the attacker can provide. Since targets act out of their volition to satisfy their desires, it is easier for the attacker to get a hold of targets passively. A very obvious example is offering money for illicit actions.

Time: "When under time pressure to make an important choice, we use a different decision strategy, and hustlers steer us toward one involving less reasoning."

This is a specification of Cialdini's scarcity principle. Time is the common resource on the line when there is scarce supply of products or services. As with the scarcity principle, Stajano explains that the lack of time makes it easier to get the target to do actions desired by the attacker.

3.4. Spear Phishing by Caputo et al.

Since the search is focused on phishing, I prepared for possible presence of special cases, like spear phishing. The definition by Caputo et al. was taken from an image in his work [7].

> "Spear phishing is a form of cyber attack attempting to infiltrate your system or organisation for cyber crime or espionage purposes. Such cyber attackers find inside information specifically relevant to you and craft fake e-mail messages, usually impersonating well-known companies, trusted relationships, or contexts."

To put it simply, it is a regular phishing attack that is augmented with personal information of the target previously gathered to increase the chance of them letting their guard down.

3.5. Other Classifications

Towards the middle of the paper I will use certain terms established and used in another paper. These are used by Intel in their effort to establish their threat agent library as a means to identify information security risks [8]. As such they are also compatible when used in context of SE, since it is closely related to information security.

- **Agent:** Refers to any entity involved in a SE attack, be they hostile or non-hostile
  - **Hostile Agent:** For the purpose of this thesis the hostile agent is the equivalent of the attacker
  - **Non-hostile Agents:** They may contribute to the attack involuntarily and, in the case of this thesis, they are also the targets
- **Outcome:** When used in connection with SE attacks, refers to the end result or consequences of the attack desired by the hostile agent

Using the examples from Section 3.1, I call the person holding the boxes the hostile agent and the one exiting the building is a non-hostile agent who actively contributes to the attack unknowingly while the desired outcome could be acquisition of business secrets or disruption of competing operations, among others. In the phishing mail example, the e-mail recipient is the non-hostile agent and whoever sent out the e-mail is the hostile agent. The desired outcome is usually financial gain.

4. Methodology

As of the 2nd of July 2015, the Juris database contained about 1.3 million court rulings. The initial set of retrieved documents only contains search results found using §263a StGB and the word "Phishing". As already mentioned at the end of Chapter 2, the search was limited to these recognisable criteria because of the assumption that jurisdiction may be already familiar with cases involving phishing, speeding up the search by quickly finding relevant court rulings thanks to a relatively high number of cases compared to other types of SE attacks. This will help keep the focus on the analysis instead of material management for this thesis. That does not mean that there are only court rulings exclusively involving these two criteria. As it turns out, many documents output by the Juris search engine are court decisions. These court decisions only document a decision regarding the application of laws made by a court, possibly to be used as reference for the future. It will be explained later in Section 5.1 that court decisions will not contain information about SE attacks.

After retrieving the documents as described above, I started the analysis by reading through every document to determine via the definitions in Section 3.1 whether they contain any SE at all and sorted them accordingly. Folders for court decisions, files that were corrupted during retrieval, court rulings containing SE and court rulings without SE were created to quickly organise the material. Whenever a court ruling contained SE I proceeded with the analysis by summarising the description inside the circumstances of a crime in a few sentences. These summaries were subsequently appended with additional information that turned out to be interesting during the analysis. As it can be taken from Table 4.1, the number of remaining documents containing SE turned out to be relatively small compared to the whole set, not to mention the number of retrieved documents compared to the total database of court rulings.

Documents	Total	§ 263a StGB	"Phishing"	Both
Total	178	119	52	7
With SE	***29***	***7***	***19***	***3***
Without SE	117	81	32	4
Court Decision	35	34	1	0

Table 4.1.: Table containing the number of documents retrieved on the 2nd of July 2015

To further categorise each document with SE I used Cialdini's principles of persuasion given in Section 3.2 and a separate set of principles that Stajano et al. identified in his research given in Section 3.3. Cialdini's principles are still regarded as very relevant for SE research and are also correlating with

Stajano's principles to some degree. Using at least two sets of principles together can help identifying characteristics that one or the other set may not have defined. I assigned one or more principles I deemed fitting for the exploited agent to the documents for the categorisation. I then began to put all crucial information into a compact table format inside an excel sheet, while also going in depth into every court document for a detailed analysis. Additional information that was thought to be relevant beforehand was already present in the table as columns before this step, including the socio-demographics of non-hostile targets, the presence of principles and the desired outcome. While reading through the documents there were recurring statements about several bits of information over all documents that were not considered before, so these were added to the table later on.

4.1. Challenges

The question whether a document contains SE can only be answered by fully reading or at least skimming through the entire document. Relevant information for the analysis is sometimes written clearly, other times hidden for interpretation. Privacy laws are applied to the documents in varying degrees that can make understanding the case description a challenge. Implicit information like the gender of non-hostile agents can be concluded by which pronouns are used if the name is kept secret. But if entire entities are replaced with one single label, for example an ellipsis, it gets difficult to follow the flow of events. This can be combined with another source of confusion: the presence of related entities to the defendant and claimant, like employees and customers if the parties are companies, even more so if the defendant and claimant are or were in a business relationship. There are many words to mix up the way the document can address each of these entities, as it was the case with the example in Section 4.2.1.

A time consuming aspect of analysing court documents is that identifying information is an iterative process. If at first you do not know what kind of information court documents may hold, you have to improvise and read through them several times while keeping notes of similarities and differences among them. Likewise, if you made a mistake and defined a data-column of which there are not many instances of information inside the documents, time will be wasted trying to find information that does not exist. The previously mentioned socio-demographics are one of them, since the documents are mostly anonymised and will not contain any data about the non-hostile agents when they are not relevant for the case.

4.2. Example Cases

Many cases that were in the search result for "Phishing" have a common set of circumstances of the crime, so I was able to group them together into which type of phishing attack was used. This type of categorising is also possible with other SE attack patterns. I am going to give a brief overview of the content of different cases.

4.2.1. Example Set 1: Common Phishing Victim

A common case of actual phishing usually involves a non-hostile agent, in this case being the financially damaged, who attempts to do his usual business using an online-banking website. Upon logging in, the agent is presented with a message allegedly displayed by the online-banking website. Many court rulings claimed at this point that the message was crafted by malicious code like trojans or malware previously installed on the agent's machine, however not stating how it got on the machine. The message content can range from a simple login error message to something sophisticated like a false claim about someone having mistakenly transferred money to this account. What all of them require in order to allow the agent to use the service again is a Transaction Number (TAN) or sets of them ranging from 10 to up to the entire page containing them. This is of course only working because all agents in these cases are still using the TAN list method for authorising transactions over the internet. The agent puts in the TANs as requested and subsequently has money transferred to an unknown bank account, since the TAN was sent by malicious code to a hostile agents for use.

Cases like these come to court with the non-hostile agent seeking compensation from the bank that manages their account, claiming that the bank is responsible for executing an "unauthorised" transaction. The agent as the claimant and the bank (or a representative) as the defendant will argue back and forth until the court comes to the decision that the claimant was either "negligent" towards their duties of keeping a safe working environment because they did not pay attention to the general terms and condition as well as security notices set up by the bank, or the bank to pay a portion or the full claimed compensation.

Example 1a: Spear Phishing

One uncommon case I came across was about a company participating in emission certificate trading [9]. The company was registered with an emission certificate trading agency and one employee in the company was assigned to managing the trading account. The hostile agent sent out an a wave of phishing mails to employees in many companies in order to obtain credentials to the trading accounts of the trading agency. The e-mail, which appeared to be sent by "Hans Frederick – www.register.dehst.de [hans.frederick@tradingprotec-tion.com]", addressed the employees with their personal names and requested them to install security updates to accommodate new security standards.

A large amount of sophisticated adjectives and technical jargon, including "128 BIT REVOLVING USB SECURITY KEY", in order to thoroughly deceive the employees. As part of the update, a link in the e-mail redirected to a website that required a verification of account credentials for the trading agency accounts. If the credentials were submitted, the hostile agent was able to submit requests to the trading agency to transfer emission certificates of affected companies to fake accounts owned by the hostile agent.

This particular case contains spear phishing as the method of attack as defined in Section 3.4. While the hostile agent still attacks multiple companies, which makes personalisation difficult, the phishing mail is written specifically to speak to the employees on a technical level of familiarity. To my understanding, that is already enough to see it as increased effort on the side of the hostile agent to gather

account credentials and tailor the phishing mail to the employees. As for which principle was used in this attack, I assigned the distraction principle from Section 3.3 to this case, because the employee's attention was diverted by the complexity of the phishing mail, hiding the fact that they are disclosing account credentials on a foreign website. Of course, it is open for discussion which principles are present, as I also believe that authority can be involved.

Example 1b: Two-step Phishing

In this case, a company Chief Executive Officer (CEO) uses the smsTAN method to authorise transactions on an online-banking website [10]. This method sends TANs to a registered mobile phone to authorise transactions. Upon logging into his account, a message interfered with the interface and notified the CEO about his account currently being unavailable. This message, like in the common case set, was produced by previously installed malicious code. When he contacted the bank about this, an employee suggested to check the firewall and reinstall the virus scanner. Following the advice, the CEO temporarily locked down his account and proceeded with the security checks. After finishing and confirming that everything was in order, he received a new Personal Identification Number (PIN) to unlock the online-banking account again. On the recent activity log, too, the CEO did not detect any irregular activities. This was not mentioned in the court ruling, but the hostile agent must have gained knowledge of the new PIN somehow in order to be able to continue the attack.

Several days later, while attending to daily online-banking business, the website displayed a message about a required security test to verify account security, due to the recent account lock-down and reactivation. The CEO pressed a button on the message to start the security test, which signalled the hostile agent to initiate an online-banking transaction using the CEO's account. This triggered a SMS to be sent to the CEO's mobile phone, containing the transaction details as well as the TAN. The SMS read: "The TAN for the transaction from 08.10.2013, 15:56:22 of 9.000,00 EUR to the IBAN *********2 is: xxx." The CEO was awaiting the TAN, as the security test required one to finish. Being steered into believing that the TAN belongs to the security test process, the CEO ignores the majority of the SMS he received and typed in the TAN into a field within the security test window. The hostile agent receives it and can proceed to finish the transaction he initiated moments ago.

This attack required, unlike the other cases, an unusually long time for the hostile agent and is an example of how security measures using personal devices can be circumvented. The principle used in this case is evidently distraction, because the CEO ignoring the SMS by being distracted with the security test played an integral part in the attack being successful.

4.2.2. Example Set 2: Common Money Mule

The second type of common cases involves the money mule as a non-hostile agent, called "leichtfertiger Geldwäscher" in German courts, with "leichtfertig" used in the sense of "thoughtless". In a variety of ways, the hostile agent manages to make contact with the non-hostile agent, who often is a retiree. Some ways include spam mails, advertisement on websites and appearing in person, the most common case being spam mail presumably because older people are not as digitally literate as everyone else. All of the technical communication channels advertise for a lucrative job as a financial manager for a

foreign company, in which the bank account of the non-hostile agent is used to transfer money as part of company proceedings and the employee may keep a small portion of the money being transferred. Contact is then established by the non-hostile agent following a link to a website set up by the hostile agent and inputting their personal information, including contact information, to apply for the job. After that the hostile agent can give instructions to the non-hostile agent as they see fit.

In reality, they transfer money from an account obtained in a phishing attack into the account of the non-hostile agent and instructs them to withdraw the money and transfer it into a foreign country using third party services like MoneyGram or Western Union. The destination of many documented transactions made by the money mule is Russia or Ukraine with further traces of the money being unavailable. The money mule is of course being assured that the job is totally legal and provided by an upstanding and foreign company.

The outcome of trials against money mules tends to lean against a guilty verdict, giving the reason that anyone should have sufficient awareness to realise that money transaction jobs like these are suspicious in nature. If the financially damaged was able to locate the money mule, then the lawsuit went directly to them.

5. Structure of German Court Rulings

Court documents usually contain a sizeable amount of "written" information about the circumstances of a crime. However, the quantity and quality of data available differs from case to case and can not be predicted without further study. Still, one can at least expect a certain order of information in German court rulings that gives the document analysis a structure. The following components may or may not be contained in a court ruling published specifically by Juris GmbH.

5.1. Head Note ("Orientierungssatz" or "Leitsatz")

The head note is located on the first page of most documents and contains the summary of particular laws to give a brief idea of what the decision might be about. One thing to note is that head notes are only added later by an editor when the document is being prepared for a publishing company; they have no legal standing. When initially analysing the documents, the head note is a good indication of whether the case at hand focuses on a crime containing SE. Sometimes, court decisions may be among the retrieved material. If that is the case, only the head note will be contained which summarises the decision. They may refer to actual rulings but they will not be on the same document.

5.2. Citations ("Fundstellen")

The citations list a number of sources in the form of abbreviations. These sources usually contain definitions of laws or norms mentioned in this ruling. As far as it concerns SE analysis, it is irrelevant.

5.3. Course of Proceedings ("Verfahrensgang")

If there are previous documents to the same case, then the course of proceedings is listed for reference. When the amount of present information is insufficient due to the current document focusing on a different aspect of the case, it may be possible to find more in the first instance of the process. A common occurrence is also the fact that the document for the first instance was not contained in the search result. It is advisable to immediately confirm presence (or absence) of SE content and divert the search for the given document accordingly.

5.4. Operative Provisions of a Judgement ("Tenor")

The operative provisions of a judgement contains the verdict and other decisions concerning the case at hand. In itself it might be interesting for other purposes but they do not contain any details regarding the case.

5.5. Circumstances of a Crime (“Tathergang”)

The circumstances of a crime is the part where one should look for descriptions of SE. There is no standard that dictates how to write it, making it time consuming to determine if the document sufficiently describes the process of a SE attack. The only exception to this is that every single statement is numbered. One thing to note when looking for SE is that most of the time, the defendant is not the hostile agent. Later during the analysis I came to the conclusion that almost all the time the defendant is an agent manipulated by the hostile agent or a third party, while the hostile agent remains unknown. Therefore, when an attack is being described, only the perspective of non-hostile agents will be available for interpretation and, by extension, analysis. Sometimes the document does not have a separate section for “the circumstances of a crime” but instead explains them inside the reasons.

5.6. Reasons (“Urteilsgründe”)

The reasons that lead up to the Tenor contains most of the discussion of various facts and details about the case and put together the evidence that justify the court’s decision. This is where much of the law citation takes place and normally does not contain details of a crime.

6. Analysis Result

At first glance, a great number of the documents are not the first instance of a case and also not the last, most prominently due to being a request of one party to review the ruling of a previous instance ("Revision" in German). If new important additional information emerges that changes the understanding of the circumstances substantially, a retrial may be ordered. The retrials can further contribute to the truth-finding process and provide new information for analysis, but only if the revision challenges the recorded circumstances of the crime. If the final verdict of a case is relevant for research, it may be necessary to continue the search through the course of proceedings of any documents that does not contain a final verdict. Otherwise, you can extract information from what is available. The following are of course not the only types of information that can be extracted from the documents. Different topics call for different kinds of information and nothing prevents the analysis to provide the related materials. This is a list of information I identified as interesting enough for further research or statistical mention.

6.1. Phishing Agent Types

One of the more obvious results is that there are three distinct types of agents as described in Section 3.5 who are present in crimes focusing on phishing: A bank customer who disclosed his online-banking account credentials and suffers financial damage, a second banking customer (the money mule) who serves as a node for money transfers and the attacker who benefits from the phishing activity. Both bank customers are non-hostile agents regarding the SE attack and the attacker is the hostile agent. The bank customers are non-hostile because their original intent was not to help the hostile agent perform the attack, even if they did end up contributing to the cause unknowingly. The outcome desired by the hostile agent is the acquisition of monetary funds. The bank (or multiple banks in case the two customers are registered to different ones) also acts as a non-hostile agent, but is not one of the main actors during the attack. Each of these agents and their relations can be seen on Figure 6.1. In order to accomplish the desired outcome, the hostile agent attacks the money mule and the financially damaged bank customer. In most cases, the hostile agent gains access to the online-banking account of the financially damaged and instructs the money mule to further transfer the money they receive through hard-to-trace means.

What then happens in the legal layer is that the financially damaged sues the bank for executing the initial transaction and, if successful, the bank (sometimes the state) consequently sues the money mule for laundering money, as they are the only available point of contact for the transaction. The reason for this is that most recipients of the money transfers are overseas. Enforcing the law of a country on entities living in different countries is a complicated matter, leaving the bank with the only financially

feasible choice of suing the money mule. The state trying to prosecute citizens of another country can have political implications as well. As a side note, there was not a single court ruling in the search result where the defendant is the citizen of a different country.

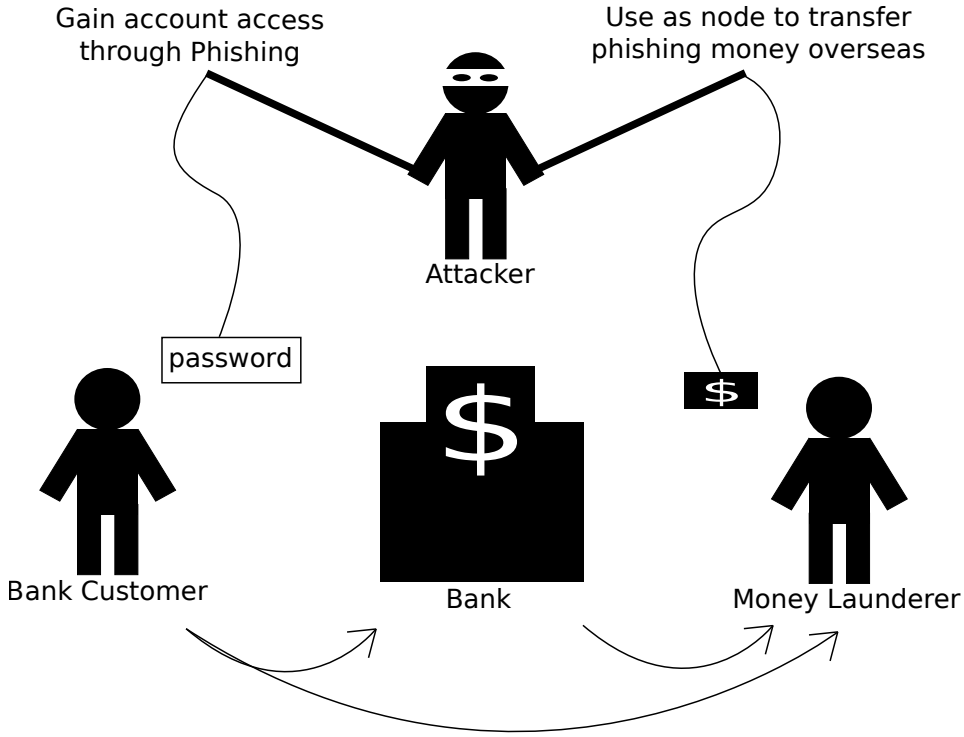

Figure 6.1.: The interactions between different agents in a phishing attack and the chain of lawsuits

For examples, refer to Section 4.2.1 and onwards. I assigned almost all of the documents in the set of cases involving the financially damaged the principle of authority and social compliance. The reasoning behind this is that the main "actors" in this case are the non-hostile agent and the hostile agent in the form of website messages. The messages displayed impose an authoritative request on the non-hostile agent to be fulfilled while usually giving no alternative to access the online-banking service. The non-hostile agent obeys the request, thinking that the program behind this is correct about its claims.

In the set of cases with the money mule a handful of different principles can come into play, depending on the current circumstances of the money mule. Most of them are actively seeking a way to improve their financial standing, making them susceptible to being exploited through the need and greed principle from Stajano. Those who were approached by the hostile agent directly were kind enough to help them out, as the agent claimed to need someone with a bank account to accept a large amount of money as a temporal measure to purchase a car. The hostile agent receives the money directly and moves it without the aid of third party money transfer services, rendering the money mule as the final trace of the phishing money. This is a case involving the kindness principle explained in

Section 3.3.

As a side-note, there is a slight possibility that phishing is misspelled in the document. A total of 5 documents from the initial search result contained the misspelling “Pishing”, which however did not have any impact on the analysis, as the correct spelling was also present.

6.2. Used Media

As the SE definition of Mouton et al. states in Section 3.1, an electronic device is involved in an attack.

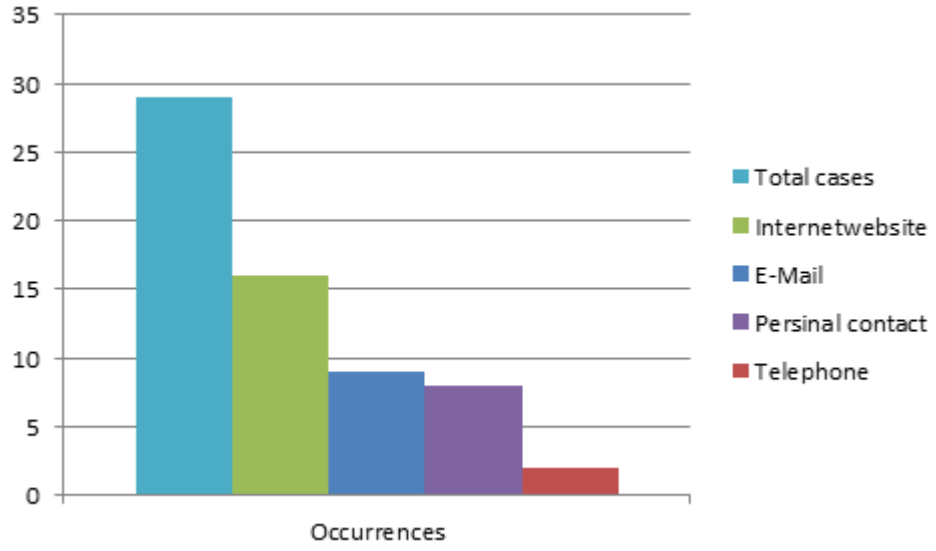

Figure 6.2.: Diagram showing the numbers of media used throughout the analysed documents

Therefore other available information I included was what kind of media was used to communicate if there was any contact. That includes phone calls, content of phishing mails or other exchanges and appearances of internet websites. Digital media like e-mail messages and internet websites are very common in technical frauds, but also unconventional approaches like personal appearances and phone calls are used in recent SE attacks. However, the contents of the conversation itself stays behind references, of which the actual documents are not available in the database. Should the need arise, there is always the option of extending the search towards them.

6.3. Time-line

When analysing dates and spans of time it is important to distinguish between multiple dates in the same document.

- The date that is written at the top of the document is the date of when the decision happened.
- The year that can be read from the case file abbreviation is the year in which the case was first submitted to law enforcement.

- The date on which the crime happened is not uniformly documented and has to be extracted from the description of the crime.

Something to keep in mind is that sometimes the year on which this document was recorded is drastically different from the year on which the first submission occurred. The analysed documents contained crimes committed in as early as 1996, the court decision for that particular case was dated in 1998, however.

6.4. Agent Attributes

Descriptions of related parties are only present on a case by case basis. Information like age and profession are still relatively common than for example nationality and main language but altogether the privacy practises will hit here the most. Hence, when trying to determine why a SE attack was successful (or not), it will most likely fall short on the victim analysis due to lack of information. Sometimes there are still situational mentions of personal information in case it was used in their defence. For example: stating that someone is not speaking German as a mother tongue, weakening the argument of not having read the terms and conditions to prevent the fraud.

6.5. Attack Process

Descriptions about the actual events are, more often than not, lacking in exact detail about how specific steps were performed. They are still enough to understand the flow of events that make up an attack. But if for example, as mentioned before in Section 6.2, information like the content of communications is needed to determine attack techniques, then court documents will not satisfy the requirement. The type of attack descriptions that can be expected from them is sufficient for a chronological reconstruction of the events. These can be used, for example, to create a framework with experiments made for re-evaluation of the attacks while filling in missing details with improvised sets of parameters.

6.6. Applied Laws

Even if the content of the documents are mostly concentrated on computer-fraud and phishing, different people have their own way of categorising the cases. Out of the 29 analysed documents, a total of 77 different laws were given in the lists of applied laws. As a matter of fact, one of the documents that were output when searching for computer-fraud do not even contain the very law for it in the list of applied laws. That leaves the possibility that SE can be found using other laws that may at first not indicate the presence of SE.

7. Conclusion

Judging by the available data, court documents definitely proved themselves to be not useless, even if the relatively small number of documents may differ from that opinion. The legal system defines an extensive library of different laws that are related in unexpected ways. A result of the majority of documents using the Phishing keyword is that the relevance of information will lean towards phishing. In this case it might overshadow some information relevant for SE research in general due to the focus shifting on details required for phishing attacks, but this can certainly be avoided with proper preparation.

Experts in internet law like Prof. Hoeren mentioned in Section 2.1 can surely provide an explanation as to which laws apply to common crimes that involve SE. I am confident that with carefully refined search parameters and different laws, additional material can be found and analysed for further research. The documents themselves are written with the best of intentions for accuracy but also privacy towards involved parties, resulting in anonymous and occasionally detailed SE attack descriptions. So in the end, research of SE attacks is possible on a case by case basis for each document, even if it not very efficient considering the ratio of SE containing documents versus SE-less documents. Additionally, they provide statistical data on SE attacks.

For further work on this topic, I suggest looking into ways to accurately extract information from court documents. The methodology in this thesis is improvised at best and can be improved on in many aspects. This should also be done in each country regardless of previous work by others, as there may be cultural differences in recording legal documents.

Also an important part is the source itself. In Chapter 2 the dark field was mentioned, the set of every crime done. From the dark field a subset is reported to the police, from which a subset is taken to court and from which again a subset is documented and published by private companies. In hindsight, the database provided by Juris GmbH provides only a small subset of cases involving SE compared to the dark field. It would drastically increase the size of available material, if access to police databases, a direct subset of the dark field, was granted.

Either way, court documents by themselves form a basic foundation for a source of information in SE research.

A. List of Acronyms

SE Social Engineering

StGB Strafgesetzbuch (penal code)

MarkenG Markengesetz (law for brand protection)

UrhG Urheberrechtsgesetz (copyright law)

TAN Transaction Number

PIN Personal Identification Number

CEO Chief Executive Officer

GmbH Gesellschaft mit beschränkter Haftung (company with limited liability)

Bibliography

[1] Kevin Mitnick et al. *The Art of Deception*. John Wiley and Sons, 2002.

[2] Frank Stajano and Paul Wilson. Understanding scam victims – seven principles for system security. *Association for Computing Machinery*, 2011.

[3] Federal Criminal Police Office. Police crime statistics, 2014.

[4] Prof. Dr. Thomas Hoeren. Internet law scriptorium, April 2015.

[5] Francois Mouton et al. Towards an ontological model defining the social engineering domain. *ICT*, 2014.

[6] Jan-Willem H. Bullée et al. The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Exp Criminol*, 2015.

[7] Deanna D. Caputo et al. Going spear phishing: Exploring embedded training and awareness. *IEEE*, 2014.

[8] Intel Corporation Timothy Casey. Threat agent library helps identify information security risks, September 2007.

[9] Landgericht Köln 3. Zivilkammer. 3 o 390/13, August 2014.

[10] Volksgericht Berlin 10. Kammer. 10 k 333.10, September 2013.