Final Thesis

E-fraud

- State of the art and countermeasures -

By

Bengt Bergman

LITH-IDA-EX--05/029--SE

2005-03-21
Final Thesis

E-fraud
- State of the art and countermeasures -

By

Bengt Bergman

LITH-IDA-EX--05/029--SE
2005-03-21

Examiner:
Associate Professor Simin Nadjm-Tehrani
Dept. of Computer and Information Science, Linköping University

Supervisor:
Professor Marc Dacier
Corporate Communications, Institut Eurécom
E-bedrägerier, situationen idag och åtgärder

E-fraud E-fraud, state of the art and counter measures

Bengt Bergman

Nyckelord
E-fraud, e-commerce, telecom fraud, fraud detection, fraud classifications
Abstract

This thesis investigates fraud and the situation on Internet with e-commerce today, to point on some potential threats and needed countermeasures. The work reviews several state of the art e-fraud schemes, techniques used in the schemes and statistics on the extent of e-fraud. This part shows that e-frauds are today both sophisticated and widespread.

Since real world frauds are deemed impossible to fully cover in order to predict potential new e-frauds, the thesis adopts a different approach. It suggests two abstraction models for fraud cases, a protocol model and a functional model. These are used to perform analysis on case studies on both telecom frauds and e-frauds. The analysis presents characteristics for both types of frauds. Using one of the abstraction models, the functional model, conceptually similar cases among telecom frauds as well as e-fraud cases are identified. The similar cases in each category are then compared, using the other abstraction model, the protocol model. The study shows that concepts from telecom frauds already exist in e-frauds.

Several challenges and some possibilities in e-fraud prevention and detection are also extracted in the comparative study of the different categories. The major consequence of the challenges is e-frauds’ higher scalability compared to telecom frauds.

Finally, this thesis covers several existing countermeasures in e-commerce along with specific countermeasures against auction fraud, phishing and spam. However, it is shown that these countermeasures do not address the challenges in e-fraud prevention and detection to a satisfactory extent. Therefore, this thesis proposes several high-level countermeasures in order to address the challenges.
Sammanfattning

Detta examensarbete undersöker bedrägerier och den nu nya situationen med e-handel, för att peka på potentiella hot och föreslå åtgärder. Det täcker de flera av senaste bedrägerierna, tekniker som används i dem och statistik på bedrägeriernas utbredning. Denna del pekar på att bedrägerierna på Internet redan är både sofistikerade och utspridda.

Eftersom alla bedrägerier i den ”vanliga” världen är omöjliga att undersöka för att förutspå möjliga bedrägerier som kan uppstå på Internet, används en annan metod i detta arbete. Två abstraktionsmodeller för bedrägerier presenteras som används för att göra fallstudier av både bedrägerier från Telecom-branschen och bedrägerier på Internet, s.k. e-frauds. Fallstudierna pekar på egenskaper för båda typerna av bedrägerier. Med hjälp av den ena abstraktionsmodellen identifieras konceptuellt lika bedrägerier från de båda miljöerna som sedan jämförs med hjälp av den andra abstraktionsmodellen. I jämförelsen dras slutsatsen att koncept från bedrägerier inom Telecom redan finns i e-frauds.

Vidare identifieras flera utmaningar samt några möjligheter i arbetet med att bekämpa e-frauds i jämförelsen. En övergripande skillnad är att e-frauds är mer skalbara än bedrägerier inom Telecom.

# Table of Contents

1  Introduction ......................................................................................... 1  

1.1  Background .................................................................................. 1  

1.2  Purpose and problem description ................................................. 1  

1.3  Description of the work ............................................................... 2  

1.4  Limitations .................................................................................. 3  

1.5  Sources of error ........................................................................... 3  

1.6  Structure ..................................................................................... 4  

1.7  Reading instructions .................................................................. 4  

2  Fraud ............................................................................................... 5  

2.1  Definition ................................................................................... 5  

2.2  Fraud classifications and taxonomies .......................................... 6  

2.3  Discussion .................................................................................. 9  

3  Telecom fraud case study ............................................................... 11  

3.1  Telecom fraud cases ................................................................. 11  

3.2  Models for abstraction ............................................................... 13  

3.3  Result ....................................................................................... 16  

4  E-fraud .......................................................................................... 19  

4.1  Definition ................................................................................... 19  

4.2  Different types of existing schemas .......................................... 20  

4.3  Techniques used in e-fraud schemas ....................................... 23  

4.4  The extent of e-fraud ............................................................... 27  

4.5  Discussion ................................................................................ 30  

5  E-fraud Case studies ....................................................................... 31  

5.1  E-fraud cases ............................................................................ 31  

5.2  Results .................................................................................... 34  

5.3  Discussion ................................................................................ 37  

6  Comparison between e-fraud and telecom fraud cases ............. 41  

6.1  Finding similar cases ............................................................... 41  

6.2  Comparison of similar cases ................................................... 42  

6.3  Discussion ............................................................................... 48  

7  E-fraud countermeasures ............................................................... 51  

7.1  E-commerce countermeasures ................................................ 51  

7.2  Other existing countermeasures .............................................. 54  

7.3  Addressing e-fraud challenges ............................................... 59  

7.4  Discussion .............................................................................. 65  

8  Conclusions .................................................................................. 67  

8.1  Answering problem description .............................................. 67  

8.2  Future work ............................................................................. 69
Appendix A – Telecom fraud case analysis...................................................... 81
  Case 1 – An old fraud .................................................................................. 81
  Case 2 – Subscription fraud ....................................................................... 82
  Case 3 – 809 telephone scams .................................................................... 83
  Case 4 – Prepaid fraud ................................................................................ 84
  Case 5 – Premium rate services fraud............................................................ 85
  Case 6 – Cloning fraud ............................................................................... 86
  Case 7 – PBX fraud .................................................................................... 87
  Case 8 – Internet Modem Switch Scam ......................................................... 88

Appendix B – E-fraud case analysis................................................................. 89
  Case 1 – Nigerian letter fraud .................................................................... 89
  Case 2 – Financial fraud ............................................................................. 90
  Case 3 – Money laundering ........................................................................ 91
  Case 4 – Internet auction fraud .................................................................. 92
  Case 5 – Business to business fraud ............................................................. 93
  Case 6 – Triangulation ............................................................................... 94
  Case 7 – Phishing ....................................................................................... 95
  Case 8 – Extortion ..................................................................................... 96
  Case 9 – Automatic bidding ....................................................................... 97
Table of figures
Figure 1: Notation for the protocol model.............................................. 15
Figure 2: Notation for the functional model............................................. 16

List of tables
Table 1: Characteristics making the telecom fraud possible based on the functional model................................................................................ 17
Table 2: Top Ten IFCC Complaint Categories 2002. Source: [10]... 27
Table 3: Amount Lost by Fraud Type for Individuals Reporting Monetary Loss 2002. Source:[10]................................................................. 28
Table 4: Characteristics of e-fraud cases based on the protocol model ............................................................................................................. 35
Table 5: Characteristics making the e-fraud possible based on the functional model.................................................................................. 36
1 Introduction

This chapter presents background, purpose and problem description, description of the work, limitations, sources of error and reading instructions for this thesis.

1.1 Background

The basic assumption of this work is that wherever money exists, fraud is also present. This has been true for decades, if not centuries. As a new economy is arising with the Internet, is it therefore quite likely that new forms of fraud will be invented. The purpose of this thesis is to identify the associated threats related to fraud in the E-business economy and to propose countermeasures.

This work has been conducted at Institut Eurecom in Sophia Antipolis, France. Institut Eurecom is a teaching and research institute in the telecommunications domain and its services. It has three departments: corporate communications, mobile communications and multimedia communications. This work has been conducted within the corporate communications department.

This thesis is in partial fulfillment of a Master of Engineering degree in Information Technology at Linköping University and covers 20 credits.

1.2 Purpose and problem description

The purpose of this thesis is to investigate fraud and the situation on Internet with e-commerce today, in order to point on some potential threats and needed countermeasures. More precisely the following problems are addressed:

1. How do instances of e-fraud currently look like?
   a. What is the definition of e-fraud?
   b. What are the state of the art e-fraud schemas?
   c. What are the characteristics of e-fraud?

2. Are there real-world fraud schemas which do not exist on the Internet and are likely to transpose to the Internet?
   a. What is the definition of fraud?
b. Are there any fraud taxonomies or classification systems which can be used to predict fraud in new environments?
c. What are the state of the art real-world fraud schemas?
d. What are the characteristics of real-world fraud?

3. **What are the differences between e-fraud and real world-fraud cases?**
a. What are the challenges in e-fraud prevention and detection?
b. What are the possibilities in e-fraud prevention and detection?

4. **What countermeasures are needed to fight e-fraud?**
a. What are the state of the art e-fraud countermeasures?
b. What countermeasures are needed to address the challenges in 3.a?

1.3 **Description of the work**

The method used in this thesis is literature studies of research articles, news, Internet and books in order to find state of the art fraud and e-fraud schemas and countermeasures. The results from the literature studies are then used in case studies where both fraud and e-fraud cases are studied and compared by using models of abstraction.

This thesis starts with an overview of existing definitions and taxonomies related to the notion of fraud. It highlights the fact that several distinct communities have shown various interests in the study of frauds. Each group has unfortunately looked at it from its own viewpoint. As a result, each approach is tailored for a given application domain and, therefore, does not offer the right elements to think about new kinds of frauds that could take place on the Internet. As a consequence, the notion of fraud is formalized in this thesis, as well as its countermeasures. This is done by means of case studies focusing on telecom frauds which is first defined in precise terms, and then rephrased in a more abstract way.

The thesis then moves on to e-fraud, and covers its definition, schemas and the situation today. A conclusion from that part is that e-fraud is already widely spread and comes in many different shapes. But in order to have a corresponding set of e-frauds to compare with
the cases from the telecom case studies and to extract the characteristics of e-fraud. 9 e-fraud case studies are presented. These cases give a picture of state of the art e-fraud schemas today. In the following comparison with the telecom fraud cases, the conclusion is that concepts from telecom frauds already are transposed to e-frauds. A set of key differences are also extracted, in terms of challenges and possibilities, existing in e-frauds but not in real world frauds. The following coverage of existing e-fraud countermeasures show that theses challenges are not addressed. Therefore, some high-level countermeasures are suggested to address them.

1.4 Limitations

As both fraud and e-fraud are widely spread, this is a big area for a thesis. Therefore, this thesis focuses on the big picture, and not in details of specific frauds or countermeasures. In the thesis several choices have been made to focus or highlight certain issues. These issues have been chosen, among others in this wide area, after careful consideration of their impact on the big picture. In other words, not all fraud schemas, not all countermeasures and not all taxonomies are covered.

In the coverage of real world frauds, the focus is on telecom fraud to make it possible to cover the area. Whether the comparison between telecom frauds and e-frauds are representative for a comparison of real world frauds and e-frauds are discussed in Section 6.3.5.

1.5 Sources of error

In this thesis two models for abstraction of fraud cases has been created. In the use of both of these models it is possible to fit a case in several ways into the models. The finally chosen layout of the cases was the result of several iterations and discussions about each model, choosing a layout that focuses on the key issues in each case. But as it is possible to make other representations of the cases, this may lead to different results.
1.6 Structure

In Chapter 2 the definition of fraud is covered along with a study of fraud classifications systems and taxonomies in order to answer problems 2.a and 2.b. To answer problems 2.c and 2.d Chapter 3 then presents case studies of telecom frauds and the abstraction models. Chapter 4 then moves on to e-fraud and covers its definition, schemas, techniques and the extent of e-fraud today in order to answer problems 1, 1.a and 1.b. But in order to answer problem 1.c (and add some material on 1.b) case studies of e-frauds are presented in Chapter 5. The following comparison between e-fraud cases and telecom cases in Chapter 6 provides answers to problems 2, 3, 3.a and 3.b. Chapter 7 then covers e-fraud countermeasures, their focus on challenges in e-frauds and proposes solutions in order to address the challenges in order to answer problems 4, 4.a and 4.b. Finally Chapter 8 summarizes the conclusions in this thesis.

1.7 Reading instructions

In order to fully grasp the content of this thesis a basic knowledge about the telecom industry, telecom services, Internet, Internet services and computer networks is needed. Without that knowledge may details in some sections and some fraud schemas be hard to understand, but it is still possible to grasp the big picture and the message in this thesis.

Knowledge about techniques used in fraud detection is not needed to understand the thesis, but certainly adds an extra dimension in terms of understanding the countermeasures. Examples of such techniques are neural networks, rule-based approaches, Bayesian nets, clustering and case-based reasoning.
2 Fraud

This chapter covers the definition of fraud, different taxonomies and classification systems in order to find tools which may be used to predict fraud in new areas.

2.1 Definition

As pointed out in Thomas et al.’s article [1] there is no single definition of fraud which is commonly accepted. Fraud is often defined within the domain of expertise of the various people proposing a definition. Several generic definitions exist for the word though. For instance, the Concise Oxford Dictionary defines fraud as follows:

“1. wrongful or criminal deception intended to result in financial or personal gain. 2. a person or thing intended to deceive.” [2]

A Dictionary of Law has the following definition of fraud:

“A false representation by means of a statement or conduct made knowingly or recklessly in order to gain a material advantage. If the fraud results in injury to the deceived party, he may claim damages for the tort of deceit. A contract obtained by fraud is voidable on the grounds of fraudulent misrepresentation.” [3]

This statement includes the consequences of the definition as an integral part of its definition. Thomas et al. [1] explain that a common idea in the various existing definitions is that the act of deception is intentional and that the act is used to gain a benefit for some part. It is worth noting that not all definitions agree with this viewpoint. For instance, in Mohay et al.’s book [4], the definition implies that a fraudster does not always need to gain anything from his misbehavior. In the context of this report, we choose to use the definition proposed by Thomas et al. [1], expressed as follows:

“Fraud is defined as a deception deliberately practiced to secure unfair or unlawful gain.” [5]

Deception and unfair or unlawful gain is defined precisely in Thomas et al.’s article [1].
2.2 Fraud classifications and taxonomies

Fraud is nothing new, even in the telecom environment. It has existed in the telecom environment since the very beginning of its existence. Examples of such frauds can be found as far back as in the 18th century [6]. In the coming sections, various classifications and taxonomies of fraud are analyzed in order to figure out if they are useful for one of the purposes of the thesis, namely the study of yet-to-be-discovered e-frauds.

2.2.1 Examples of classifications of general fraud

In Thomas et al.’s article [1], the authors, after having surveyed the literature, decide to propose their own decision tree to classify frauds. The most common types of fraud are grouped into 8 different categories, using the relationship between the victim and the fraudster as a discriminating factor. The categories can be summarized as follows:

- **Consumer fraud** – A member of the public is being deceived.
- **Plagiarism** – An academic is using someone else’s work without crediting them.
- **Occupational fraud** – The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.
- **Client-Supplier fraud** – The client is an organization who deceives the supplier.
- **C-2-B fraud** – A client to a company claims something which is false in order to get some benefit from an organization.
- **Academic misconduct** – The fraudster acts as an academic and claims something which is not true in order to get benefit from an organization.
- **Public duties evasion** – By providing false information or hiding information you avoid a public duty, for example tax.
- **Outsider attack** – Frauds suffered by an organization, perpetrated by a party they have no explicit relationship to.
The decision tree is not detailed enough to be used as a classifier for all types of fraud. Even though the foundation of the decision tree is independent of the techniques used, a classification which can be used to predict new frauds has to consider more than eight different kinds of frauds.

In Mohay et al.’s book [4], the authors split all frauds between Internal and External ones, depending on the fact that the fraudster is a member of the organization which is the victim of it or not. They then give examples of groups of each kind though they do not attempt to cover all kinds of fraud.

The Federal Trade Commission (FTC) maintains a database called Consumer Sentinel [7] in which they store consumer fraud and identity theft complaints. This database received in 2003 516,740 complaints (in 2002 404,000). The database stores complaints according to the following categories:

- Advance Fee Loans and Credit Protection/Repair Offers
- Business Opportunities and Work-at-Home Plans
- Foreign Money Offers
- Health Care
- Identity Theft
- Internet Auctions
- Internet Services and Computers
- Investments
- Magazine and Buyers Clubs
- Multi-Level Marketing/Pyramids/Chain Letters
- Offices Supplies and Services
- Prizes/Sweepstakes and Lotteries
- Shop-At-Home/Catalog Sales
- Telephone Services
- Travel, Vacation and Timeshare Plans
- Other complaint categories

These categories are more a clustering of existing cases then a well though-through categorization and can therefore not be used as a general classification of frauds.
2.2.2 Examples of classifications of internal fraud

The Association of Certified Fraud Examiners (CFE) [8] has a classification system which is called *Uniform Occupational Fraud Classification System*, commonly known as The Fraud Tree. This classification system is very detailed but it covers only *Internal fraud*¹. The classification system contains 70 entities and CFE uses the classification system to classify the frauds they examine. The classification system is more extensively described in CFEs annual report from 2004.

The classification system is based on the method used by the perpetrator. There are three major classes: *Asset Misappropriation*, *Corruption* and *Fraudulent Statements*. Among them, the *Asset Misappropriation* class is the largest one with 45 sub entities. *Corruption* has only 10 sub entities while *Fraudulent Statements* has 12. CFE [8] also points out that there are frauds which can not be placed into a single entity. For instance, they mention several cases that belong to both *Corruption* and *Asset Misappropriation* classes.

Since the Fraud Tree is detailed and has a clear criterion for what diverges different classes, it is a good start for a classification system. But the fraud tree is specific for internal fraud and can therefore not be used for every type of fraud. Another drawback is that a single case of fraud can fit into several classes.

2.2.3 Examples of classifications of online fraud

The Internet Fraud Complaint Center’s (IFCC) reports [9] [10] use nine categories to group the complaints they receive regarding online frauds. These groups are described in Section 4.2. This classification is interesting for the purposes of the thesis as it already considers online frauds. However, as explained in Thomas et al.’s article [1], this approach is not well suited when it comes to classifying new types of frauds. Indeed, some classes presented there come from a description of the victim, namely the ones named *Financial Institution Fraud*, *Gaming Fraud, Communications Fraud, Utility Fraud, Insurance Fraud* and

---

¹ CFE refers to *Internal fraud* as *Occupational fraud*, but in this document *Internal fraud* will be used.
Government Fraud. On the other hand, another class, Business Frauds, describes who the fraudster is. The remaining classes, Confidence Fraud and Investment Fraud, look at the problem from a perpetration method viewpoint: breaching a relationship of trust; receiving investments under false pretences or stock market manipulation. As a consequence, mixing classification criteria like this makes new specimens harder to classify. Finally, the method to classify a specimen is not made explicit leading to the risk of seeing a given fraud type being assigned to different classes by different users of the approach.

2.2.4 Examples of taxonomies

In Vasiu and Vasiu’s article [11] a taxonomy for computer frauds is offered. It uses two criterions to classify fraud cases, namely the perpetration platform and the perpetration method. The perpetration platform, describes how the perpetrator managed to get access to the required resources to perform the fraud: either with or without authorization. The perpetration method describes how the attack itself has been perpetrated: either by means of data or thanks to a program.

This taxonomy is considered in Thomas et al.’s article [1] as a possible starting point for a real world taxonomy, but is discarded on the basis that determining if someone has exceeded its authorization or has acted without authorization can be a very difficult problem. It is also hard to classify a fraud which has mixed perpetration platforms. The taxonomy is also clearly designed to deal with computer intrusions rather than with frauds, in the general sense.

2.3 Discussion

As seen in Section 2.2 there are several different approaches among the classification systems and taxonomies. However, none of them offers the properties required for classifying all kinds of fraud in a non ambiguous way. Combining the existing methods into one might be an option. But experience shows the difficulty and the limits of this approach because of the diversity of the goals pursued by each methodology. As a result, another solution is presented by this thesis. Starting from a set of representative fraud cases, they are simplified,
identifying their key components and abstracting the underlying principles of all these fraud cases using a common notation.
3 Telecom fraud case study

In this chapter, case studies of telecom fraud are presented. The case studies aims at finding groups of telecom frauds and characteristics, by analyzing the cases using abstraction models, also presented in this chapter.

3.1 Telecom fraud cases

All cases presented here are fictitious but representative of real schemes that are known to have taken place. The case descriptions used when conducting the study were longer and more detailed than here, where only the basics in each fraud case are presented.

Case 1 – An old fraud

In the 19th century the telegraph was introduced. But all the bookmakers did not use it on order to get the result from the racetracks. It was then possible, by using a helper who was at the race track, to get the result using the telegraph, in order to place a bet on the winner before the bookmaker got the result by courier. This case is based on a case described in Petticrew’s article [6].

Case 2 – Subscription fraud

This case is based on getting a cellular phone with a contract without intention of paying for it. The fraudster gets the subscription and the telephone for $1 or similar and uses a false identity when signing the contract. The fraudster then uses the contract to forward international calls which the fraudster is selling to a cheap price. An additional profit is made by selling the telephone on the black market. This case is based on the techniques for subscription fraud and call selling operations described in Kvarnström et al.’s article [12] and how the subscriptions is made is from Veeneman’s article [13]

Case 3 – 809 telephone scams

The fraudster calls in this case private persons and leaves a message on their answering machine, asking them to call a number to get information about a relative who is in the hospital after an accident. The number is a Premium Rate Services number which is more
expensive then an ordinary number and the extra expense goes to the fraudster and the fraudster’s telephone operator. The case is based on a press release from the Fraud Control Association [14] and several cases in ICSTIS’s report [15].

**Case 4 – Prepaid fraud**

In this case an employee at a telephone operator notes codes from vouchers used for refilling prepaid telephone cards. The fraudster then uses the codes to refill its friend’s telephone card. The persons who later on buy the already used vouchers can not use them to refill their cards (since the vouchers already have been used), but they are compensated by the operator when showing the receipt. This case is based on the description of un-authorized refills in Subex Systems’ white paper [16].

**Case 5 – Premium Rate Services fraud**

In this case the fraudster sets up a company which opens a service with highly charged Premium Rate Services numbers. When people are calling to these numbers the company and the telephone operator split the income with each other. But when the telephone operator sends bills to the phone numbers which have called the PRS-number, none of them are paid. That is because the fraudster has used cloned telephones and telephones achieved under false identities to call to the PRS-number to generate income. This case is based Premium Rate Services fraud described in Kvarnström et al.’s article [12].

**Case 6 – Cloning fraud**

In this case a private person’s SIM-card is stolen and cloned. As the SIM-card is returned the private person does not notice that it was stolen. The fraudster then uses the clone to make calls from abroad. The private person refuses to pay for these calls, and the telephone operator has to pay the telephone operator abroad according to their roaming deal. This case is based on the descriptions of cloning and roaming fraud in Kvarnström et al.’s article [12] with additional information from the real world case described in Batino’s article [17] and smart card details from 3G.co.uk’s press release [18].

Case 7 – PBX fraud

In this case a Private Branch Exchange (PBX) is hacked by the fraudster. A PBX is a telephone switchboard for managing a company’s telephone lines. The fraudster controls it after it has been hacked so that the fraudster is able to forward incoming calls to abroad and thus only paying the cost for the telephone calls to the company. The fraudster uses this to sell calls to abroad, letting the company pay for the calls. This case is based on the call forwarding case in Petticrew’s article [19], with details about accessing PBXs from Hodgson’s white paper [20].

Case 8 – Internet Modem Switch Scam

In this case a person browsing a porn website downloads a program which is supposed to let him watch the pictures. The program redirects the modem to a PRS number owned by the fraudster without noticing the person using the computer. The case is based on a case described in FTC’s press release [21], but there are details from cases in ICSTIS’s report [15].

3.2 Models for abstraction

The models presented in this section were used in the case analysis to make the abstraction of the cases.

3.2.1 Protocol model

In the case studies, interest is focused on abstracting the flow of communications between the various parties involved in each case. In other terms, the “protocol” runs by the various entities in order to make the fraud a success.

To describe the cases, 4 different types of communicating entities are used:

- **Fraudster** – The one who commits the fraud
- **Victim** – The victim of the fraud
- **Insider** – An entity that can gain access to important information thanks to his/her position in the victim’s organization.
• **Outsider** – An entity who is neither a fraudster, nor a victim, nor an insider.

In the model, the following writing conventions are used to refer to the various types of message exchanges taking places between the entities:

• **MP x** - *Make Proposal x*, the proposal x is presented to another part  
• **AP x** - *Accept Proposal x*, the proposal x is accepted  
• **RP x** - *Reject Proposal x*, the proposal x is not accepted  
• **CP x** - *Commit Proposal x*, the part does whatever proposal x demands or allows the part to do  
• **SI** - *Send Information*, the part sends some kind of information to another part  
• **TI** - *Take Information*, a part takes some kind of information from another part, without the other part knowing  
• **GV** - *Give value*, a part gives some value (for example money) to another part

The direction of the events are straightforward, but it should be clarified that for TI the arrow representing the communication goes from the one who takes the information to the one it is taken from.

In the model, there are also three different kinds of important moments during the run of such protocol which are identified, namely:

• **PD** - *Possible Detection*, at this point is it possible to detect fraud  
• **VR** - *Victim Realizes*, at this point does the victim realizes it is a victim of a fraud  
• **PAYS** , At this point does the victim loses value of some kind because of the fraud

The notation for the protocol is shown in Figure 1.

The different motivations for the events and the explanation of the proposals are explained case by case. The communication events are presented in chronological order with the first one being on the top
and the last one in the bottom. There is no semantic attached to the vertical distance between two arrows.

Figure 1: Notation for the protocol model

3.2.2 Functional model

The protocol model shows a case’s characteristics and pinpoints some points which are important for the fraud and how these are conducted. But the model is not abstract enough to find the concepts in the cases. Therefore the functional model was developed, which goes one step further in the abstraction by looking at values. The protocol model can point out similarities in the process of committing the fraud, and the functional model can be used to focus on actors and values. With its higher level of abstraction it aids detecting differences between fraud cases. The model makes it possible to identify concepts in the frauds, which are not connected to techniques.

The model describes how values are transferred among the roles. Each value is represented by a letter; x, y, z, etc. and the relationship among values are shown by functions, F, F’, F’’ etc. For example if y is a function of x, that is simply written by y = F(x). The arrow which describes the first value transfer comes first, and the arrow describing the last value transfer comes last. The notation for the model is depicted in Figure 2.
The model is used to analyze what happens to x, y and F during a fraud. If a value is expected but not delivered it is shown in the model with a branch that is labeled with a cross. This very simple notation enables us to highlight various classes of frauds.

**Figure 2: Notation for the functional model**

### 3.3 Result

The representations of the cases in the models are in Appendix A – Telecom fraud case analysis. In the analysis of the cases the analysis of the protocol model representations focused on finding characteristics of the frauds and the functional model analysis focused on finding characteristics which makes the fraud possible for the fraudster.

#### 3.3.1 From the protocol model

A major conclusion from the protocol model is that there is in many cases (cases 2, 3, 5-8) a repetitive part which should be minimized in order to minimize the costs of the fraud. How this part can be minimized differs from case to case. There are in all cases at least two possible points of detection, hence there are always more than one way to discover a fraud. In cases 4 and 5 there is also a possibility for the fraudster to spread the cost of the fraud (and the possibility to detect it) on several different positions by generating a lot of different small incomes to itself, but still generate a large income in total.
Another conclusion is that it is common that the victim pays for the fraud after the fraudster has got its income (case 3, 4, 6-8).

### 3.3.2 From the functional model

*Table 1: Characteristics making the telecom fraud possible based on the functional model*

<table>
<thead>
<tr>
<th>Case</th>
<th>Hiding expense</th>
<th>Changing probability</th>
<th>Non-delivery</th>
<th>Impersonation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Old</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 – Subscription</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>3 – 809</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 – Prepaid</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>5 – PRS</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6 – Cloning</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>7 – PBX</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>8 – Modem</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1 displays which characteristics which make the fraud possible to commit for the fraudster based on the functional model. The characteristics are the following:

- **Hiding expense** – In these cases F in the functional model is changed without the victims’ knowing. F is changed so that the victims have to pay more than they are aware that they have to pay for.

- **Changing probability** – In these cases is F in the functional model changed so that the probability of paying to the fraudster is bigger in a gambling or similar situation. This is done without the victims’ knowing.

- **Non-delivery** – In these cases the fraudster makes sure that y is not provided, when x has been received in the functional model. In other words, the fraudster makes sure that payment or delivery of value is cancelled.

- **Impersonation** – In these cases the fraudster attacks x in the functional model. The basic notion is that the fraudster uses
something which belongs to someone else in order to make the actions look like they are made by that someone, and also to make sure that someone is responsible for paying.

As seen, all parts of the function model, F, x and y, are altered, hidden or attacked in some way in order to create a fraud. In cases 1, 3 and 8 F is attacked, in cases 2 and 5 y is attacked and in cases 4, 6 and 7 x is attacked. In the cases where the attack is on F, the fraudster always starts by transporting a value of some kind (x) to the victim. In the cases where the attack is on y the schema begins with the fraudster getting a value. This is natural, since if the fraudster has begun with giving a value, the fraudster wants to change the rules (F) for the value returned in order to make a profit or it wants to change the value received (x). If the fraudster has gotten a value, the fraudster does not want to pay for it, hence the attack is on y.
4 E-fraud

In this chapter is e-fraud defined for the further use in this thesis. Different types of e-fraud schemas are explained along with some techniques used in the schemas in order to give a picture of state of the art e-frauds. Finally the current extent of e-fraud is presented. This chapter does not cover all type of e-frauds, but the ones considered as most widespread and/or interesting.

4.1 Definition

By looking at how the term e-fraud is used today it can be seen that there is no general definition of e-fraud. KPMG uses e-fraud as a fraud which is related to e-commerce in a survey of e-fraud [22]. In a document from the law firm Taylor Wessing the term e-fraud is used as a synonym for computer fraud [23]. Western Economic Diversification Canada uses the notation of e-fraud as a synonym to online fraud. [24]

Internet Fraud Complaint Center (IFCC) uses the notation Internet fraud for fraud committed over the Internet [10] and in the fraud complaint database Consumer Sentinel a fraud complaint is said to be Internet-related if it concerns an Internet product or service, the company initially contacts the consumer via the Internet or the consumer responds via the Internet. [7]

Because of the ambiguous use of the notation e-fraud and the use of Internet fraud and Internet-related fraud synonymously this thesis presents a new definition of e-fraud based on the definition of fraud introduced in Section 2.1 and the notation of the most famous “e-word”: e-mail. This new definition will be used in this thesis.

The Concise Oxford English Dictionary defines e-mail as:

“Messages sent electronically from one computer user to one or more recipients via a network. The system of sending e-mail.” [25]

By combining the definition of e-mail with the definition of fraud from Section 2.1 the following definition is created:
“E-fraud is defined as a deception deliberately practiced to secure unfair or unlawful gain where some part of the communication between the victim and the fraudster is via a computer network and/or some action of the victim and/or the fraudster is performed on a computer network.”

4.2 Different types of existing schemas

In IFCC’s report [10] regarding complaints received about fraud on the Internet there are nine different categories used to categorize the frauds. The categories are the following:

- **Confidence Fraud** – A fraud where the trust on another person or party results in financial loss. Auction fraud, Nigerian letter fraud and non-delivery fraud (see later in this section) are members of this category.

- **Financial Institution Fraud** – A fraud against a business, organization or other that manages money, credit or capital. Credit/debit card fraud and check fraud (see later this section) are members of this category.

- **Gaming Fraud** – This fraud involves risking something of value, typically money, in order to win something but the odds or events are manipulated. This category includes for example monitoring the network of a gaming site to see other players’ secrets [26].

- **Business Fraud** – A fraud when an organization knowingly misrepresents the truth or conceals a material fact in order to gain some value. This category includes when a company provides false (positive) information about their products or similar on their website.

- **Investment Fraud** – A fraud which uses capital to generate more money in a deceptive way. This category includes manipulating stock prices by spreading false information through Internet bulletin boards and by sending e-mails. The fraudster then uses the rise or the fall of the stock to generate profit.

- **Communications Fraud** – A fraud against the systems which exchange information using different forms of media. This category includes unauthorized reselling of bandwidth using an ordinary Internet connection.
• **Insurance Fraud** – A fraud in the relationship between an insurance company and its customers. This category includes for example cases where doctors use the Internet to get in contact with patients having HIV. The doctors then validate them as healthy on their insurance papers, so that they get life coverage when the disease is “discovered” [27].

• **Government Fraud** – A fraud against the government in order to get some benefit. This category includes tax evasion when the tax forms are filled out online [1].

• **Utility Fraud** – A fraud against a government regulated public service such as electricity or water supply.

The IFCC statistics [10] use the following more specific categories as well (these categories are subcategories of the above described ones):

• **Auction fraud** – A fraud conducted on an Internet auction website. This category includes cases where a fraudster sells something via an auction website, receives money for it but does not send the buyer any goods.

• **Nigerian letter fraud** – A fraud where an e-mail is sent from an “official” representing a foreign government or agency. The letter presents a business proposal where a large amount of money is transferred into the recipient’s personal account (for one reason or another) and the recipient is offered a percentage of the transferred money. But the fraudster asks the victim to send some money before the transfer in order to pay some banking fees, taxes or similar and after the money is transferred to the fraudster, the fraudster disappears. [9]

• **Non-delivery** – A fraud where someone buys an item on a website and pays in advance. The company responsible for the website takes the money but does not send the buyer the goods.

• **Credit/debit card fraud** – A fraud where someone uses stolen (or in other illegal ways achieved) credit/debit card numbers to buy goods or services online.

• **Check fraud** – A fraud where someone uses a false check to buy goods or services online.

Phishing [28] is a type of e-fraud where someone is fooled to give away personal financial data (credit card numbers, account numbers,
pin codes, passwords etc) to the fraudster. The victim is convinced to give away the data through spoofed e-mails and fraudulent spoofed websites where trusted brands are used. For further technical information about spoofing, see Section 4.3.1.

Online extortion [29] [30] is an e-fraud based on a threat which is presented to a company. The company is asked to pay a sum of money to the fraudsters, otherwise the fraudsters will expose the company’s website to a denial of service (DoS) attack. For further technical information about DoS attacks, see Section 4.3.3.

A fraudster can collect credit card numbers by using false merchant sites [31]. On these sites the victims are offered free or very cheap services, and the victims are asked to provide their credit card details in order to pay for the services or for verifying age or similar for a free services. The credit card details are later on used by the fraudster.

A sophisticated type of e-fraud is triangulation [32]. In this type of fraud the fraudster operates from a website which offers goods at heavily discounted rates and the goods are also shipped before payment. The site appears to be legal. The customers must provide name, credit card number etc. when buying. When the customer makes an order, the fraudster orders the same product (in the name of the customer) from another, legal, website with stolen credit card details. After a while the credit card details from the customer is used to buy goods, both to the fraudster and to other customers of the fraudster’s website (that is, buying goods from another website which the customers has ordered from the fraudster’s website). The purpose of this fraud is to cause a lot of confusion in order to buy some time for the fraudster’s website to operate on and collect credit card numbers.

Business to business fraud [33] is an e-fraud schema where a company or an organization uses the Internet to commit fraud against other companies or organizations. This is possible due to the systems used in e-commerce. A company (the fraudster) can for example neglect to update price reductions on their products in automatic systems which companies (the victims) use to buy goods from the fraudster’s company using the Internet. The victims will not notice that they are being over charged unless they manually compare the prices to the market prices.
Internal fraud [1] is another type of e-fraud. An employee can for example steal information from a workplace by e-mailing the information to a personal e-mail account. Plagiarism and academic misconduct can also be conducted using the Internet. In these cases the fraudster uses information found on the Internet and either claims that the information is from the fraudster or uses the information in a different context and thereby alters its meaning.

It is also possible to do money laundering using the Internet [34]. Gambling websites provides a big opportunity for a money launderer. Money can be laundered by for example opening an account on a gambling website, put in some dirty money, gamble for a small amount of them and then withdraw the remaining amount. Thereby a legitimate source (a gambling website) is provided for the dirty money. If an owner of the gambling website is in cooperation with money launderer, the person can also loose the whole amount on the gambling website, providing a legitimate income for the owner of the gambling website.

### 4.3 Techniques used in e-fraud schemas

There are more techniques than mentioned here which are used in e-fraud schemas mentioned in the previous section, but the techniques covered in this section are considered as the most important and/or interesting. Spoofing will be covered because it is used in order to fool the victims in different contexts and to hide the attackers identity, worms are covered because they are used to create botnets and spread malicious code (for example key loggers), denial of service attacks are covered because they are used as a mean of power by the fraudsters and virtual browsers are covered because they let the fraudster commit frauds automatically on the Internet. This section aims at giving some knowledge to the reader about these hacking techniques, if this knowledge already exists, please proceed to Section 4.4.

#### 4.3.1 Spoofing

Spoofing occurs when a misleading context is created in order to fool the victim [35]. There are different kinds of spoofing, in this section e-mail spoofing, website spoofing and URL spoofing are covered.
E-mail spoofing is when the e-mail address of the sender of the e-mail is changed to a false e-mail address, hence the e-mail appears to be from someone else [36]. This can easily be done by changing the settings in an e-mail program.

Website spoofing is when a website tries to fool its visitors into believing that the website represents a known brand or organization [35]. The attacker can make the website look and feel like the original website in order to fool the victim. There are also scripts which generate a pop-up window in front of the real website, hence the victim believes the real website has generated the pop-up window [37]. Cross-site scripting (XSS) [38] is another technique which can be used to create a misleading context. XSS is when a user enters something on a dynamic webpage, for example a forum, and the entry contains some kind of malicious code of some kind, attacking the other users who browse the website. XSS can be used to enter a link to a phishing site on a known brand’s website.

URL spoofing is when displayed URLs look like URLs of known brand [37]. This is often used to redirect the victim to a spoofed website. A link entered in HTML can easily have a different goal than the URL showed because of the semantics of the a-tag in HTML. The tag “<A HREF="http://www.fraud.com">www.trusted.com</A>” would show the link www.trusted.com but it would direct the user to http://www.fraud.com. The URLs showed in browsers’ address and status bars can be changed using different techniques. It is also possible to use a real URL which is similar to the URL of another website. For example is www.liu.edu.se similar to www.liu.se.

4.3.2 Worms and botnets

A computer worm is a program that self-propagates across a network exploiting security or policy flaws in widely-used services [39]. A worm discovers new machines to exploit by scanning the network, by having a predefined targets list, by exploring an infected computer in order to find addresses of new victims or by waiting for computers to contact the worm. A worm can propagate by transmitting itself during the infection process, by using a secondary channel to transmit the worm after the infection process has been completed or by embedding itself as a part of a normal communication channel by
either appending to or replacing normal messages. The payload of a worm is the code carried by the worm apart from the propagation routines and the code is limited only by the goals and imagination of the attacker. Worms can for example be used to set up botnets and to format hard drives.

A botnet is a network of interconnected bots\(^2\), where a bot is a compromised host which is controlled via an Internet Relay Chat (IRC) channel[40]. IRC is an Internet protocol which allows people anywhere on the Internet to join real-time text based discussions [42]. Botnets are used to coordinate different types of attacks. The IRC channel is used by the attacker to control the bots. Typically the bot is an executable file spread by a worm which can perform some given actions depending on the orders provided by the attacker on the IRC channel. Botnets can be used for DDoS attacks, installations of key loggers or other Trojans on infected machines, controlling machines (backdoors) and to store illegal data. Botnets can also be used for sending spam [43], thus hiding the origin of the attacker. Botnets are rented and sold on the black market to private persons or illegal organizations.

### 4.3.3 Denial of service attacks

A denial of service (DoS) [44] attack is an explicit attempt by an attacker to prevent legitimate users of a service from using some resources.

A well-known attack is the Smurf attack [44]. In this attack the attacker sends a large amount of Internet Control Message Protocol (ICMP) echo traffic to a set of Internet Protocol (IP) broadcast addresses. The source addresses of these ICMP-packets are spoofed with the victim’s IP-address as their source addresses. Most hosts reply to the source address with an echo reply. Since there might be hundreds of hosts receiving the echo message on each broadcast address, the victim will receive a lot of traffic.

\(^2\) Bots are also called zombies or drones. [41]
The SYN-flood attack is another well-known attack based on the TCP three-way handshake [44]. In this attack a lot of SYN-packets (synchronize/start) are sent to a machine. When a host receives a SYN-packet it returns a SYN/ACK-packet (synchronize/acknowledge) and waits for a final ACK-packet (acknowledge). The attack is based on not sending the last ACK-packet, hence the attacked host will wait for a lot of ACK-packets and become unable to process new incoming connections.

Another attack is the UDP flood attack [44]. This attack is based on the UDP echo and character generator services provided by most computers on a network. The attacker uses forged UDP-packets to connect the echo service on one computer to the character generator service on another computer. The result is that the two services enter an infinitive loop and, by doing so, can be driven into a situation where they consume all available bandwidth between the computers.

A distributed denial of service (DDoS) attack [44] is a DoS attack executed from a lot of different computers. This makes the attack more difficult to prevent. The DDoS attack uses many attack daemon agents on different computers, these agents perform the actual attack on the victim and are not on the attacker’s computer. The attacker has compromised these computers and in some way installed the attack daemons there (see Section 4.3.2 about worms and botnets). The attack daemons are controlled by a control master program which coordinates the attack. The control master program is also installed on a computer which does not belong to the attacker. The attacker contacts the control master program and gives the program a command in order to start the attack.

4.3.4 Virtual browsers

In the press release from the U.S. department of justice [45] about the verdicts on the hackers Gorshkov and Ivanov it is mentioned that the hackers used programs which automatically interacted with websites and created both e-mail, PayPal and eBay accounts. The programs also created auctions and did bidding and paying on eBay.

The possibility of programs interacting with web services is investigated further in Byers et al.’s article [46]. They show that by using some hundred couple of lines of Perl code, a program can
automatically submit a form on a website. In their article they focus on an attack where a program automatically searches the web for forms where a catalog can be ordered, and then the program tries to submit these forms with a specific address, either attacking a private person or a certain post office. They use this as an example of an attack against the physical infrastructure.

As shown in Ahn et al’s article [47] the ability for computers to automatically perform actions online has been used to for example manipulate online polls and to automatically create e-mail accounts.

### 4.4 The extent of e-fraud

**Table 2: Top Ten IFCC Complaint Categories 2002. Source: [10]**

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auction Fraud</td>
<td>46.1 %</td>
</tr>
<tr>
<td>Non-delivery (mdse and payment)</td>
<td>31.3 %</td>
</tr>
<tr>
<td>Credit/debit Card Fraud</td>
<td>11.6 %</td>
</tr>
<tr>
<td>Investment Fraud</td>
<td>1.5 %</td>
</tr>
<tr>
<td>Business Fraud</td>
<td>1.3 %</td>
</tr>
<tr>
<td>Confidence Fraud</td>
<td>1.1 %</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>1.0 %</td>
</tr>
<tr>
<td>Check Fraud</td>
<td>0.5 %</td>
</tr>
<tr>
<td>Nigerian letter Fraud</td>
<td>0.4 %</td>
</tr>
<tr>
<td>Communications Fraud</td>
<td>0.1 %</td>
</tr>
</tbody>
</table>

There is no statistics on the total cost of e-fraud, but some exist for subsets of them. Consumer sentinel [7] received in 2003 166,617 complaints on fraud and identity theft which were Internet-related. The total amount paid in these complaints was $199 million. The average amount paid in each complaint was $1,341 and the median amount paid was $195. IFCC [10] received in 2002 75,063 complaints
about fraud in the U.S. of which 90% were related to the Internet or online services. The total dollar loss in these complaints was $54 million. The average amount paid in each complaint was $1,482 and the median amount paid was $299. Both IFCC and Consumer Sentinel are based on the customer filing a complaint and both do not try to do any estimation of the total amount or cost of e-fraud.

As seen in Table 2 auction fraud was the most common complaint in 2002. According to Consumer Sentinel [7] auction fraud was the most common Internet-related fraud in 2003 as well, representing 48% of the Internet-related complaints.

Table 3: Amount Lost by Fraud Type for Individuals Reporting Monetary Loss 2002. Source:[10]

<table>
<thead>
<tr>
<th>Complaint type</th>
<th>% of Complainants Who Reported Dollar Loss</th>
<th>Average (median) $ Loss per Typical Complaint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auction Fraud</td>
<td>87</td>
<td>$320</td>
</tr>
<tr>
<td>Non-delivery</td>
<td>82</td>
<td>$176</td>
</tr>
<tr>
<td>Credit/debit Card Fraud</td>
<td>62</td>
<td>$120</td>
</tr>
<tr>
<td>Investment Fraud</td>
<td>75</td>
<td>$570</td>
</tr>
<tr>
<td>Business Fraud</td>
<td>75</td>
<td>$220</td>
</tr>
<tr>
<td>Confidence Fraud</td>
<td>58</td>
<td>$1,000</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>15</td>
<td>$2,000</td>
</tr>
<tr>
<td>Check Fraud</td>
<td>56</td>
<td>$1,100</td>
</tr>
<tr>
<td>Nigerian letter Fraud*</td>
<td>&lt;1</td>
<td>$3,864</td>
</tr>
<tr>
<td>Communications Fraud</td>
<td>36</td>
<td>$174</td>
</tr>
</tbody>
</table>

* Of 16,164 complaints, 74 individuals lost money totaling $1.6 million

As seen in Table 3 the fraud with the highest median loss in 2002 is Nigerian letter fraud, followed by identity theft, check fraud and
confidence fraud. But after these 4 categories there is a big gap before the next category in terms of losses. Luckily, the four categories with the highest median loss are not the most common complaints. As seen in Table 2 the most common of them is confidence fraud, which stands for 1.1 % of the total amount of frauds.

CyberSource’s [48] annual survey of 348 online merchants in North America from 2004 says that online merchants lose 1.8 % of their revenues due to online payment fraud. This means a total estimated amount of $2.6 billion in North America, without counting indirect costs. Among these companies 5.9 % of the orders are rejected due to suspicion of fraud, and of the accepted orders 1.4 % turn out to be fraudulent.

Gartner Research [49] estimates the cost of phishing during 2003 to $1.2 billion for U.S. banks and credit card issuers. They also estimate that 30 millions of the U.S. population has been victims to a phishing attack during 2003 and estimate that another 27 million have received what “looked like” a phishing attack. The Anti-Phishing Working Group (APWG) [28] says there were 1974 unique phishing attacks in July 2004. A unique attack is defined as a single e-mail blast sent out at one time, targeting one company or an organization, and having one unique subject line. The most common companies to be attacked in July 2004 were Citibank (682 attacks in July 2004), U.S. Bank (622), eBay (255) and Paypal (147).

Gartner Research [50] estimates that $700 million was lost in online sales in 2001 because of credit card fraud in the U.S. This represents 1.14 % of the total annual online sales of $61.8 billion. The corresponding rate for offline sales were 0.06 % in 2001. It is also important to notice that in the U.S. merchants pay for the online credit card frauds [51] [52]. The card issuers demand that all fraudulent transactions made by a merchant should be compensated (often with a penalty fee) by the merchant.

Alan Paller, the director of research at the SANS (SysAdmin, Audit, Network, Security) Institute, estimates that 6,000-7,000 organizations are paying online extortion demands [29]. He also says that it is very common that online gambling web sites are paying fees to extortionists.
An example of the dynamic of e-fraud is that after the terrible disaster with the tsunami in Asia on 26 December 2004 a series of related fraud occurred on the Internet [53]. Within days of the disaster websites claiming to raise money for the victims appeared (but the money went to the fraudsters) and e-mails were sent as spam where attached files claimed to show pictures of the disaster area but instead contained malicious code.

4.5 Discussion

In Section 4.2 it is shown that many different types of e-frauds exist. That fact, combined with the statistics in Section 4.4, clearly states that e-fraud today is widely spread and exists in large scale on the Internet. The techniques used in the schemas (Section 4.3) show together with the schemas that e-frauds today also are both sophisticated and organized. This chapter does however not give any information about the characteristics of e-fraud. So in order to investigate the characteristics and be able to compare them to the telecom fraud characteristics from Section 3.3, case studies of e-frauds are presented in the next chapter.

In the investigation of e-frauds and their extent some e-frauds are found more common and widespread than others. Therefore, considering this chapter, the countermeasures in Chapter 7 covering e-fraud countermeasures will focus on e-commerce countermeasures (protecting online purchases from fraud), countermeasures against auction fraud, countermeasures against phishing fraud, countermeasures against spam and preventive countermeasures in general. The focus on e-commerce countermeasures is because credit cards involvement in many e-fraud schemas, auction fraud and phishing fraud are focused on because they are very common, spam is focused upon because it is used in many frauds to contact the victim and preventive countermeasures are focused on because they can protect against many types of e-frauds.
5 E-fraud Case studies

In this chapter, case studies of e-fraud are presented. The case studies aim at investigating characteristics of e-frauds, by analyzing the cases using the abstraction models from Section 3.2. This chapter also presents a foundation for the comparison between e-fraud and telecom cases in Chapter 6.

5.1 E-fraud cases

All cases are fictitious but representative for real schemes that are known to have taken place. The case descriptions used when conducting the study were longer and more detailed than here, where only the basics in each fraud schema are presented.

Case 1 – Nigerian letter fraud

In this case the victim gets an e-mail from a person saying he is a Nigerian government official. There is a proposal in the e-mail about transferring a large amount of money through the victim’s account, leaving some money on the victim’s account. The money that should be transferred has been forgotten on a Nigerian government account for a long time because of an overpayment. When the victim agrees, an e-mail is sent asking for some money in order to arrange some last few things. After the victim has paid the money to the fraudster, the fraudster continues to ask for more money until the victim gets suspicious, and then the fraudster disappears. This case is based on the description of the Nigerian Letter Scam in IFCCs report from 2001 [9] and there are some details from the Internet Scambusters’ web site [54].

Case 2 – Financial fraud

In this case, Internet bulletin boards are used to spread a rumor about a company in order to increase the demand of the company’s stocks. The fraudster spreading the rumor has bought stocks in the company before the rumor is spread and when the stock price rises because of the increasing demand, the fraudster sells its stocks making a big profit. This case is based on the description of the pump and dump
schema in Investopedia.com’s Online Investments Scams Tutorial [55] with details from Painter’s bulletin [56].

Case 3 – Money laundering

In this case the fraudster launders money by opening an account at a gambling website. The dirty money is put on the account using a PayPal account and then some money is spent on gambling. But the money remaining after the gambling is transferred to another, ordinary, bank account providing a legal income for the money, gambling. This case is based on the description of money laundering using a gambling website done by Malcolm [34].

Case 4 – Internet auction fraud

In this case a person buys a computer on an Internet auction website, after winning the bidding. The seller (the fraudster) contacts the buyer when the auction is finished and demands the money up front, before the delivery. The buyer agrees and transfers the money, but the computer is not delivered by the seller. This case is based on the description of the Teresa Smith case in IFCCs report from 2002 [10].

Case 5 – Business to business fraud

In this case two companies set up an automatic system for delivering and paying of goods between each other. The payments are automatically done by the system over the Internet, letting the two companies’ business systems talk to each other. The fraud is then conducted when the company which delivers the goods neglects to update the prices, which they should do according to the deal, when the market prices for the goods drop. So overcharging occurs for a long time before this is by an accident discovered by the other company. This case is based on a description of a similar case in an article in Computerworld [33].

Case 6 – Triangulation

In this case the fraudster puts up a website letting people believe it is an ordinary and legal, but cheap, website selling computers. It does not demand the money until the computers are delivered, but it still takes the credit card details during the purchase. The purchases are then conducted by ordering the computers from a different more
expensive website using previous customers’ credit card details. The victim’s credit card details are in this case not used in a fraudulent manner until some time after the purchase, making it harder to understand the origin of the fraudulent use. This case is based on the description of triangulation in Sylvester’s website on credit card fraud [32] with details about credit card repayment from Lang’s article [52].

Case 7 – Phishing

In this case the victim receives an e-mail from what appears to be the victim’s ISP. The e-mail asks him to update his username, password and credit card information. The victim follows the link and the ISP’s website appears with a pop up window in front of it. The information entered by the victim in the pop up window is received by the fraudsters and soon they begin using the victim’s credit card details. This case is based on FTC’s description of a phishing case in a press release [57]. But some technical details are from APWG’s report on phishing from June 2004 [57]. The details about the credit card transactions repayment are from Lang’s article [52].

Case 8 – Extortion

In this case an online betting site receives a threat by e-mail that if they do not pay a certain amount to a certain account, their website will be exposed to a DDoS attack. This case is based on the cases described in Astor’s article [59].

Case 9 – Automatic bidding

The fraudster has in this case access to a large amount of credit card numbers. The fraudster then uses a program that automatically creates e-mail accounts with random names, opens accounts for transferring money on the Internet connected with an e-mail account and a credit card number and then finally opens e-bay accounts connected with the other accounts. When creating the e-mail accounts, the program needs to enter digits from a picture. This is done by forwarding the pictures to people wanting to become members at the fraudster’s porn site, which then enters the digits believing they have done it in order to become member on the porn site, not knowing they have helped the fraudster to create e-mail accounts. The program then automatically bids for semiconductors
and buys them, delivering them to a postbox near the fraudster’s home, providing income to the fraudster. This case is based on the case with e-Bay and PayPal described in a U.S. department of justice press release [45] and with some details from Byers et al.’s article [46]. The details about the credit card transaction repayments are from Lang’s article [52]. The man in the middle attack used to get the digits is described in Stubblebine and Oorschot’s article [60].

5.2 Results

The representations of the cases in the models are in Apendix B – E-fraud case analysis. In the analysis of the cases the analysis of the protocol model representations focused on finding characteristics of the frauds and the analysis of the functional model representations focused on finding characteristics which make the fraud possible for the fraudster.

5.2.1 The protocol model

Table 4 displays different characteristics of the e-fraud cases based on the protocol model. The characteristics are the following:

- **Simple** – A case is considered as simple if it has 3 or fewer proposals.
- **P-2-P** – (Private to private) A fraud is considered as private to private if both the fraudster and the victim(s) in the case are private persons.
- **Repetitive part** – A case has a repetitive part if the case contains a repetitive part which accumulates the cost for the victim.
- **Hide ID** – A case has this characteristic if the fraudster hides its real identity in some way during proposal communication.
- **Mountable** – A case with a repetitive part (mountable cases are a subset of repetitive cases) and it is possible for the fraudster to make each repetitive part consider a small amount. More important, it is also possible for the fraudster to do the repetitive part a lot of times, to mount up the total profit.
**Table 4: Characteristics of e-fraud cases based on the protocol model**

<table>
<thead>
<tr>
<th>Case</th>
<th>Simple</th>
<th>P-2-P</th>
<th>Repetitive part</th>
<th>Hide ID</th>
<th>Mountable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Nigerian</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2 – Financial</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3 – Mon. laund.</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>4 – Auction</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>5 – B-2-B</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6 – Triang.</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7 – Phishing</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>8 – Extortion</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9 – Aut. bidding</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case</th>
<th>Not committing</th>
<th>Message detection</th>
<th>Behavior detection</th>
<th>Non-human detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Nigerian</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 – Financial</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>3 – Mon. laund.</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>4 – Auction</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 – B-2-B</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6 – Triang.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7 – Phishing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>8 – Extortion</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9 – Aut. bidding</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- **Not committing** – A case has this characteristic if the fraudster does not commit a proposal in order to get profit of some kind.

- **Message detection** – A case where one or more points of detection are based on recognizing the fraud from the origin or the content of a message.
• **Behavior detection** – A case where one or more points of detection are based on recognizing fraudulent behavior based on the fraudster’s actions.

• **Non-human detection** – A case where one or more points of detection are based on identifying that a human is not performing the actions.

### 5.2.2 The functional model

*Table 5: Characteristics making the e-fraud possible based on the functional model*

<table>
<thead>
<tr>
<th>Case</th>
<th>Hiding expense</th>
<th>Changing probability</th>
<th>Non-delivery</th>
<th>Impersonation</th>
<th>Using system</th>
<th>Creating circumstances</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – Nigerian</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 – Financial</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 – Mon. laund.</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 – Auction</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 – B-2-B</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 – Triang.</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 – Phishing</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 – Extortion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9 – Aut. bidding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Table 5 displays which characteristics which make the fraud possible for the fraudster to commit based on the functional model. The first four characteristics are explained in Section 3.3.2, the last two are explained here:

• **Using system** – In these cases the fraudster does not attack any part of the functional model, hence it uses the system as it is to generate the fraud.

• **Creating circumstances** – In these cases F is created by the fraudster. That means that in a normal case F should not be possible but in the fraudulent case F is created.

Since the characteristics making the e-fraud possible in Table 5 allows only one for each e-fraud case, these characteristics will be used to
group frauds cases into classes in the comparison in Chapter 6 in order to map similar telecom cases to e-fraud cases.

5.3 Discussion

In this discussion the results presented in Section 5.2 will be discussed. There will be a discussion based on the protocol model focusing on the consequences of the characteristics, both for the fraudster and the countermeasures. There will also be a discussion based on the functional model which identifies different groups of frauds and also discusses how these characteristics can be removed.

5.3.1 The protocol model

As seen in Table 4, the fraudster never committing its part of a proposal makes fraud possible in some cases. That means that in those cases the victim has committed its part of the proposal but does not get the favor returned. This problem can in general be avoided by using trusted third parties, committing the proposal at the same time etc. This characteristic can in other words, if wanted, be avoided.

It can be seen in Table 4 that it is common that there is a repetitive part which accumulates the fraud cost for the victim. This part should be minimized in all of these cases and it is important, when considering protection against a fraud, to identify this part which accumulates the cost. As seen, this repetitive part can in more than half of these cases be used to mount up several small fraudulent profits to a big one. This can be used by the fraudster in order to avoid being discovered, since many fraud detection systems use thresholds of different kinds and the fraudster can stay under the thresholds using this opportunity. Small frauds are also in general harder to detect since the difference compared to non-fraudulent actions is smaller. Thus the fraudster can stay under the thresholds and not be caught but still generate a big profit.

An interesting observation is that all private person to private person cases in Table 4 are also considered as simple. This fact combined with the fact that all of these cases can be detected by doing research on the content and the origin of messages implies that in these cases is it relatively simple for a private person to detect the fraud if he/she
knows what to look for. In other words is it very important that private persons know how to find out that these messages may lead to a fraud, although the assumption that every user is capable of this can never be true.

Finally Table 4 shows that the fraudster uses the possibility to hide its identity in every case except one. This implies that the fraudsters are very interested of staying anonymous during the frauds. This makes it of course harder to find the fraudster when (if) the fraud is discovered. It also makes the common detection method of looking at the content and the origin of a message harder, since although the origin is known, does it not provide any information about the identity. The detection of fraudulent content or origin of a message is also hard to do automatically, since in many cases the degree of truth must be analyzed which is a very difficult task for a computer program. A computer program can however discover similar messages if the same type of message are used several times in different frauds.

5.3.2 The function model

The different characteristics needed for making the fraud from Table 5 provides a good classification for all types of frauds. The classification is based on which part of the functional model (or no part) which is attacked and what the basic notion of the attack on the part is. Because of this foundation, the classification is not connected to a certain area of frauds and can be used to classify all types of frauds. The names of the classes are based on the basic property which makes the fraud possible for the fraudster. This section discusses the possibility of removing this property.

In “Hiding expense” and “Changing probability” F is attacked. The possibility to protect F is easy as long as F is controlled by an honest service (for example if F is how much goods you get from an online merchant for a certain amount of money), but otherwise it is a difficult task because if F is probably dependant on a lot of things which may be affected by the fraudster. In for example e-fraud case 2 (financial fraud) the basic notion of F (the stock market) is that it is not controlled by anyone. Instead it is controlled by the demand of stocks. However, changing F in order to make it harder for the
fraudster to attack might not be popular with the non-fraudulent customers, since F might be dependant on the service.

In “Creating circumstances” F is attacked as well but in order to stop this class of fraud one must remove the possibility to create an F for the fraudster. How this can be done differs from case to case.

For the class “Non-delivery” several known countermeasures exist. Trusted third parties can receive both x and y in order to make sure both values get delivered to both parties and that they fulfill the demands, the part providing x can also often decide on its own whether or not to deliver x before it gets y.

In order to stop frauds of the class “Impersonation” strong means of verification of the identity must be provided, to make it hard for the fraudster to act as somebody else and thereby being able to attack x.

In the class “Using system” no part of the model is attacked as opposed to the other classes. This means that in this class the environment, as it is, provides all the necessary characteristics that the fraudster needs to commit the fraud. Therefore, in order to make it harder for the fraudster to commit this type of fraud one must change the environment or provide effective means of detecting the fraud. Naturally, these environments should be avoided to the largest extent, but avoiding such an environment may include shutting down a service for non-fraudulent users.
6 Comparison between e-fraud and telecom fraud cases

This chapter presents the results of a comparison between the telecom fraud cases and the e-fraud cases. The purpose of the comparison is to display differences between the two groups of cases and also to see if there is any type of telecom fraud schemas which has not been transposed to the world of the Internet.

The comparison presented here uses the functional model to find conceptually similar cases and compares these cases using the protocol model to find differences. In this chapter are cases are initially mapped to groups of conceptually similar cases based on the functional model. Then the groups of conceptually similar telecom frauds and e-fraud cases are compared based on the protocol model. Finally the differences are summarized and discussed focusing on the consequences of the differences. Various groups are also discussed.

6.1 Finding similar cases

By comparing the result from the functional model case studies from telecom and e-fraud cases in Section 3.3.2 and Section 5.2.2 a natural grouping of telecom and e-fraud cases appears. Four of the listed characteristics from the functional model are in common among the studied cases for telecom frauds as well as for e-fraud. The characteristics are:

- Hiding expense
- Changing probability
- Non-delivery
- Impersonation

These characteristics are used to form the groups of telecom and e-fraud cases within which these cases will be compared.

The fact that the characteristics “Using system” and “Creating circumstances” do not have any telecom case representation is discussed in Section 6.3.4.
6.2 Comparison of similar cases

In the comparison of the cases belonging to the same classes in Table 1 and Table 5 the protocol model is used to compare the e-fraud cases with the telecom cases. The cases are compared by comparing the possible points of detection (PD), how the fraudster is communicating with the victims during making (MP) and acceptance (AP) of proposals, how the fraudster commits (CP) its proposals, and how the fraudster sends information (SI). These isolated events are compared because the points of detection tells how hard it is to detect the fraud and the fraudsters actions tells how hard it is for the fraudster to commit the fraud and thereby also shows the scalability of the fraud from the fraudster’s point of view. This section presents the result of this comparison by presenting the cases in each group and their differences. The differences are summarized at the end of this section.

6.2.1 Hiding expense

This group includes e-fraud case 5 (Business to business fraud), telecom case 3 (809 telecom scams) and telecom case 8 (Internet modem switch scam). These cases are all similar in that they hide an extra expense (higher price or calling a premium rate services number) without the victims knowing. This is seen by the attack on F in the functional model.

By comparing the protocol model representations of these cases, the following differences can be seen:

- **Automation** – In the e-fraud case, business to business fraud, the final detection of the fraud is very late compared to the telecom cases because all information needed to detect the fraud is within the automatic system and thereby non-reviewed. In the telecom cases the frauds are detected when the telephone bills arrive.

6.2.2 Changing probability

This group includes e-fraud case 2 (Financial fraud) and telecom case 1 (An old fraud). These cases are all similar in that the fraudster changes the possibility of the victim to pay to the fraudster
(manipulating the stock market or knowing the result of the race) without the victims knowing. This is seen by the attack on F in the functional model.

By comparing the protocol model representations of these cases, the following differences can be seen:

- **Anonymity** – It is easy for the fraudster to stay anonymous during proposal communication in the e-fraud case since it can use a username on the Internet bulletin board. This is harder in the telecom case since the person sending the telegraph must show up physically to do this.
- **Fraud cost** – When sending information in the e-fraud case, the cost is negligible (Internet bulletin boards). But there is a fee in the telecom case for sending a message using the telegraph.
- **Speed** – In the e-fraud case the proposal communication is faster from the fraudster’s point of view since a web service is used to buy stocks, while the communication is done face to face in the telecom case.
- **Ubiquity** – The fraudster can be anywhere in the world when committing the proposals in the e-fraud case, while it must be done face to face in the telecom case. It is also possible for the fraudster to act as several users using different usernames in the e-fraud case, while doing this in the telecom case demands many good physical disguises.
- **Lack of interconnection** – In the e-fraud case, financial fraud, it is hard to use the point of detection based on detecting the pattern, because it is not likely that different bulletin boards and the stock market cooperate and are interconnected. This makes it hard to connect bulletin board users to stock market users and other bulletin boards users. This is not the case in the telecom fraud, the old case, since bids must be delivered face to face.
- **Interpretation** – It is easier to interpret the data in the points of detection in the e-fraud case since it is in written text, compared to speech in the telecom case.
- **Available data** – In the e-fraud case all the data are saved automatically in the bulletin board which makes it easier to
analyze the data in the points of detection compared to the telecom case where the dialogues need to be recorded.

6.2.3 Non-delivery

This group includes e-fraud case 1 (Nigerian letter fraud), e-fraud case 4 (Auction fraud), telecom case 2 (Subscription fraud) and telecom case 5 (premium rates services fraud). These cases are all similar in that the fraudster does not deliver a promised value. This is seen by the attack on y in the functional model.

By comparing the protocol model representations of these cases, the following differences can be seen:

- **Anonymity** – It is easier for the fraudster to stay anonymous during proposal communication in the e-fraud cases because of the anonymity in auction website accounts and e-mails. This is harder in the telecom cases because of the use of identity cards and the face to face communication.

- **Available victims** – It is easier for the fraudster to reach a lot of victims during proposal communication in the e-fraud cases using the auction website’s advertisement and spam. In the telecom cases is this harder because of the face to face communication.

- **Fraud cost** – The proposal communication is cheaper (negligible cost) in the e-fraud cases because of the use of e-mails and auction website services. In the telecom cases parts of the communication are face to face which introduces costs of traveling to the fraudster.

- **Speed** – The proposal communication is faster in the e-fraud cases because of the use of e-mails and auction website services. These services are faster than the face to face communication. The proposal committing (sending some e-mails) is also faster in the e-fraud cases compared to the telecom cases (physical writing of papers).

- **Ubiquity** – Some points of detection based on patterns are harder to use in the e-fraud cases since a user may have several usernames and act as a crowd (having several users at the auction website or several e-mail addresses), which is not possible in the telecom cases.
• **Novel users** – In the e-fraud cases some points of detection are based on validating if something is true, for example the information about an auction item or the origin of an e-mail. There is a high risk in the e-fraud cases that this detection is done by novel users, who not are used to validating what is true and not true on the Internet, thereby making them likely to miss the points of detection. The corresponding detection in the telecom cases are performed by companies which should be experienced in that field.

• **Interpretation** – It is easier to interpret the data in the points of detection in the e-fraud cases (e-mails, biddings etc) since it is in written text, compared to speech in the telecom cases (dialogues, phone calls).

• **Available data** – It is easier to collect data in the points of detection in the e-fraud cases (e-mails, biddings etc) compared to the telecom cases (dialogues, phone calls).

### 6.2.4 Impersonation

This group includes e-fraud case 6 (Triangulation), e-fraud case 7 (Phishing), e-fraud case 9 (Automatic bidding), telecom case 3 (Prepaid fraud), telecom case 6 (Cloning fraud) and telecom case 7 (PBX fraud). These cases are all similar in that the fraudster uses something (credit cards, vouchers or SIM-cards) which belongs to someone else in order to make the actions look like they are made by that someone, to make him/her responsible for paying. This is seen by the attack on x in the functional model.

By comparing the protocol model representations of these cases, the following differences can be seen:

• **Anonymity** – It is easier for the fraudster to stay anonymous during proposal communication in the e-fraud cases using e-mails and websites compared to using telephones as in the telecom cases.

• **Automation** – In the e-fraud cases triangulation and automatic bidding the proposal committing is performed automatically by a program while it has to be carried out manually in the rest of the cases.
• **Available victims** – It is easier for the fraudster to reach many victims in the proposal communication in the e-fraud cases using e-mails and websites. The corresponding technique in the telecom case is telephones.

• **Fraud cost** – In the e-fraud cases the proposal communication is cheaper (negligible cost) using e-mails and websites compared to the communication using telephones in the telecom cases.

• **Speed** – The proposal communication is faster in the e-fraud cases using e-mails and websites compared to telephones used in the telecom cases.

• **Ubiquity** – Some points of detection in the e-frauds can not be used in the same way as in the telecom frauds. In the cloning telecom case one can for example use a SIM-card in two different places within a certain interval of time leading to an easy detection of the fraud but on the Internet everybody can use services at different websites simultaneously, without any interval in between. The SIM-card also provides an identifier for one single person which can be used to investigate patterns in that persons behavior, but since there is no cost in creating numerous users at the different Internet services, one person can have several usernames in the e-fraud cases. The possibility of using IP-numbers as substitute for a SIM-card exists, but since the use of bots is widespread among fraudsters is it not likely to help to any great extent.

• **Novel users** – Some points of detection are more likely to be successful in the telecom cases because a larger part of the users are familiar with the telecom services compared to the Internet services and can detect the signs of different frauds.

### 6.2.5 Summary of differences

Summarizing the comparison in the groups the following challenges with e-fraud prevention and detection compared to telecom fraud prevention and detection exist:

• **Anonymity** – Anonymity in web services lets the fraudster hide his/her identity more easily than in telecom cases during proposal communication, committing and sending of information in e-fraud cases. It also makes it easier to act as
someone else in proposal communication in e-fraud cases. Finally it makes some points of detection harder to use in e-fraud cases compared to telecom cases because it is harder to connect events to users in pattern matching.

- **Automation** – It is easier for the fraudster to commit proposals in e-fraud cases compared to telecom cases because of different techniques letting this be done automatically. Automation also makes possible points of detection in e-fraud cases harder than in telecom cases since they are in the automatic part.

- **Available victims** – It is easier for the fraudster to reach many victims in the e-fraud cases compared to the telecom cases during the proposal communication and sending of information because of the possibilities of different web services.

- **Fraud cost** – It is cheaper for the fraudster to communicate during proposals in e-fraud cases compared to telecom cases because the negligible cost of many web communication services.

- **Speed** – Both proposal communication and proposal committing are faster for the fraudster in many e-fraud cases compared to telecom cases because of the different web services used.

- **Ubiquity** – It is harder to detect fraud patterns in the possible points of detection in e-fraud cases because one user can have several usernames in web services and it is hard to detect that these usernames are connected. This is not the case in telecom services. In telecom services geographical facts can be used to detect fraud in possible points of detection, but ubiquity makes this hard in e-fraud cases. Ubiquity makes it easier for the fraudster to act as a crowd when sending information in e-fraud cases because it is easy to get several usernames and use them simultaneously in web services than telecom services. Finally ubiquity makes it easier to commit proposals in e-fraud cases because they can be committed from anywhere in the world.

- **Lack of interconnection** – In e-fraud cases some points of detection are harder to implement than in telecom fraud cases because different web services are not connected and
therefore is it not possible to find patterns in the use of these web services.

- **Novel users** – In the points of detection in e-fraud cases it is harder for the victims to discover the fraud because they are to greater extent novel users, which are inexperienced in using the services.

Summarizing the comparison in the groups the following possibilities with e-fraud prevention and detection compared to telecom fraud prevention and detection exist:

- **Interpretation** – In the points of detection in e-fraud cases is it easier to interpret written text automatically then spoken words which often is the case in telecom cases.
- **Available data** – It is easier to collect data for the points of detection in the e-fraud cases since the data is often automatically saved in different web services.

### 6.3 Discussion

In this discussion the major consequence of the challenges and the specific consequences of the challenges “Anonymity” and “Ubiquity” are discussed. Furthermore the mapping of telecom cases to the classes containing e-frauds is discussed along with the fact that two classes do not contain any telecom frauds. It is also discussed whether or not the result here can be seen as a representative for a comparison between real world frauds and e-frauds.

#### 6.3.1 The major consequence of the challenges

All challenges derived from the comparison in Section 6.2 except “Novel users” and “Lack of interconnection” makes it easier for the fraudster to communicate during proposals and commit proposals more easily. The major difference between telecom and e-frauds is therefore that the e-fraud cases are more scalable from the fraudster’s point of view in both finding and dealing with victims. The scalability of the schemas is very frightening, especially when considering the characteristic “Mountable” from Section 5.2.1 and that private person to private person cases are considered as “Simple” (Section 5.3.1) along with the challenge “Novel users”.
6.3.2 Consequences of “Anonymity”

The challenge “Anonymity” brings a lack of trust to other parties on the Internet. The lack of trust comes from the anonymity and can be explained by comparing a business deal with a person made face to face, and making the business deal with a person shouting to him on the other side of a high, thick wall and then throwing the money and the goods over the wall to each other. The anonymity also contributes to making it hard to connect law enforcements when the fraud is detected.

6.3.3 Consequences of “Ubiquity”

There is a legal consequence of the challenge “Ubiquity” because when a fraud is discovered, it might be the case that the fraudster is on the other side of the world and the country it is operating from may have different laws than the country of the victim. This implies that pressing charges against the fraudster are in many cases complicated and expensive (even though you know the identity of the fraudster). Therefore is it likely that the victim does not press charges in many cases, especially if the fraud considers a small value.

6.3.4 Mapping of telecom cases to the classes

As seen in Section 6.1 all telecom fraud cases are conceptually similar to an e-fraud case. The conclusion is that the concepts from telecom fraud schemas are already transposed to the Internet. Telecom fraud cases can therefore not be used to predict new concepts in e-fraud schemas which are likely to occur on the Internet.

The classes “Using system” and “Creating circumstances” do not have any telecom fraud representation. The fact that “Using system” does not have it is believed to be because in the telecom environment only services exist, but on Internet there are both services and values. There are on the Internet merchants, banks, payment services, casinos etc which have introduced values (or money) on the Internet. These kinds of services dealing with real values do not exist in the telecom world and therefore the class “Using system” can not be found there. The fraudster must introduce some kind of values in the telecom world in order to make the fraud possible.
The fact that “Creating circumstances” does not have a telecom cases is believed to be because Internet is possible to change (e.g. make a website etc) for a private person, while in the telecom world the private person can only use the services as they are. Thereby is it easier for the fraudster to generate the circumstances needed to create the fraud on the Internet.

6.3.5 Real-world fraud aspect

The differences derived here between the telecom fraud cases and e-fraud cases are considered as representative differences between real-world frauds and e-frauds. This is because the telecom environment has proved prone to contain frauds for a long time and it uses techniques which are firstly not used on the Internet and secondly cover many different aspects of how fraud can be done in the real world (providing false ID, hacking PBX, internal fraud etc).

However, it is not possible to conclude that real world fraud concepts in general already are transposed to the Internet, since telecom fraud concepts are. There are unfortunately no proofs that there are no other concepts in other fraud domains in the real world. Before that conclusion can be made, all real-world fraud domains must be investigated. But considering the large extent of e-fraud shown in Section 4.4 is it not judged as reasonable to cover all domains of real world fraud in order to answer this question. Telecom cases are, however, believed to represent a majority of the concepts, since frauds have a long history in the telecom environment.
7 E-fraud countermeasures

This chapter presents e-fraud countermeasures by covering countermeasures used in e-commerce and the most interesting countermeasures addressing e-frauds in other areas. A study of how these countermeasures address the challenges from Section 6.2.5 is presented along with proposals for addressing the challenges. This chapter is finished with a discussion about the need of standards among countermeasures and consequences of some proposed solutions.

7.1 E-commerce countermeasures

7.1.1 Real world methods

In some cases similar techniques are used both for Internet and the real world countermeasures. In credit card fraud detection systems rules, risk scoring and neural networks technologies are used for both online and offline transactions, since both types of transactions can occur on the same account. [31]

7.1.2 Manual reviews

Manual reviews [48] of incoming orders are used by a majority of online merchants. Manual reviews involve a person who checks if an order is fraudulent or not by using different methods. Studies show that 19 orders can on average be reviewed per hour by one employee. Manual review techniques [61] involve for example checking customer records, calling the customer, calling the bank, e-mailing the customer using positive and negative lists and consulting publicly available services.

7.1.3 Guarantees

A countermeasure to provide the customer and the merchant with a feeling of safety is to have a third-party who provides a guarantee for a transaction to both the merchant and the customer. Worldpay [62] and Fia-Net [63] are two examples of companies that provide this service. The merchant gets this guarantee for its customers and itself
if the merchant’s system fulfills certain criteria, for example having a fraud detection system provided by the company providing the guarantee. Merchants participating in the service have an icon showing on their website that the transaction is guaranteed by the third-party company. The idea is to increase the customer’s feeling of safety. The third-party company then covers costs for both the merchants and their customers if there is a fraud.

7.1.4 Credit/Debit card verification

There are different methods used on Internet in card-not-present transactions (when somebody manually provides the credit card details without physically showing the card) to verify that it is the actual owner of a credit/debit card which enters the information [31]. One method uses a 3 or 4 digit number code printed on the card but not available on the magnetic stripe. The merchant asks the customer to provide this code with the purpose of ensuring that the customer is in actual possession of the card. Hence, people who only have copied the information on the magnetic stripe can not provide this information. Different card issuers have different names to indicate this security feature: CVV2 for VISA, CVC2 for Master Card and CID for American Express.

Another method used in card-not-present transactions is Address Verification Service (AVS) [31] which matches the first digits of the street address and the ZIP code information given for delivering/billing of the purchase with the corresponding information the card issuer has on record. A code representing the level of match between these addresses is presented to the merchant. Existing AVS systems are not accurate in international transactions.

7.1.5 Payer authentication with 3-D Secure

3-Domain Secure (3-D Secure) [64] is an authentication protocol which is developed by Visa for online credit card transactions. Visa’s brand identity for this protocol is Verified by Visa (VbV) and MasterCard has also developed a protocol based on 3-D secure called MasterCard SecureCode.
3-D Secure [65] is based on a three-domain model. In the Issuer domain the credit card issuer is responsible for managing the enrollment of their cardholders in the service and authenticating cardholders during online purchases. In the Acquirer domain the acquirer is responsible for providing the transaction processing for authenticated transactions and for defining procedures which ensure that the merchant participating in the Internet transactions has an agreement with the acquirer. The Interoperability domain provides a common protocol for the other two domains and shared services in order to enable safe transactions between them. The model allows an owner of a credit card to use a personal code or some other shared secret in order to make purchases on the Internet with the credit card.

7.1.6 Fraud detection

ClearCommerce’s fraud detection system FraudShield [66] for card-not-present transactions uses lockout mechanisms, negative and positive lists, fraud rules and risk scoring to detect fraud. Lockout mechanisms are used to detect customers which are potentially fraudsters and then refusing them when they try to perform a transaction. A customer can be locked out when there is a big amount of declined transaction (a fraudster is trying to find a valid credit card number) from the same card number, the same source IP or the same customer ID. Lockout mechanisms can however sometimes lockout legitimate customers. Negative lists are card numbers, e-mail addresses etc which are used to identify possible new frauds. A card number used in a fraud can for example be saved in a negative list. Positive lists are used to identify trusted customers. Fraud rules are used to create rules which identify known frauds based on different kinds of data in the transactions. Risk scoring is a method used to generate a score between 0 and 100 which indicates how likely it is that the current transaction is fraudulent. Risk scoring is implemented using neural networks trained on a large set of Internet transactions.

CyberSource and VISA provide a fraud detection system called CyberSource Advanced Fraud Screen enhanced by VISA [67]. The system calculates a risk score for every card-not-present transaction. The risk score is based on comparing the transaction to thousands of high and low-risk profiles based on account, merchant, transaction...
and global data. The actual computation is done by combining neural networks and a rule-based approach.

Quova [68] provides a feature which can be used by merchant websites. Their software GeoPoint provides the merchant with the location of the computer (based on the IP-address). The merchant can then use this information to compare it with for example the shipping address. The system provides the opportunity to highlight suspicious transfers, in order to not block out legitimate customers e.g. shipping goods to family members abroad.

7.1.7 Statistics on used e-commerce countermeasures

According to CyberSource’s survey among online merchants in 2004 [48] a median of 5 fraud management tools are used by each merchant. The most popular countermeasure is Address Verification Service, used by 82 % of the online merchants. Card verification numbers (CVV2, CVC2 etc.) are second most popular and used by 56 % of the merchants. Then internally-built fraud screens/decision models, customer history and negative files follow around 50 %. Geolocation is used by 31 % and finally commercial fraud screening/risk scoring services, card association payer authentication services (Verified by Visa, MasterCard SecureCode etc) and consortium/public records database are all used by around 25 %.

The survey [48] also investigates what countermeasures the merchants are planning to use. Card association payer authentication services are most popular with 31 % planning to use it followed by geolocation (22 %) and commercial fraud screening/risk scoring services and card verification numbers (both 19 %).

7.2 Other existing countermeasures

7.2.1 Preventive in general

E-frauds are prevented to a large extent by providing customers with information about possible frauds. FTC [69] has a lot of information on their website to show customers how to protect themselves against e-fraud. Service providers provide information to their customers on how to avoid being exposed to fraud [70]. There is also
information available for merchants on how to avoid fraud. The website AntiFraud.com [71] offers for example information to merchants on how to minimize the risk of fraud when using online payment.

There are a lot of technical preventive countermeasures [72]. Secure socket layer (SSL) can be used to protect sensitive information, firewalls can be used to protect internal networks and data storages, virus scanning software can be used to protect against viruses, existing security patches should be used to update used software etc.

There are also organizational measures [22] which can be taken to prevent e-fraud. Background checks can be made on entities which support and assist a company and their e-commerce system. Security audits can be performed on e-commerce systems. Seals can be used on websites to identify that the system has passed a security audit. Separation of duties can be introduced to the maintenance of an e-commerce system. Response procedures can also be prepared in case of a security breach in an e-commerce system.

7.2.2 Auction fraud countermeasures

To prevent online auction fraud identity verification, secure payment mechanisms, escrow services, feedback rating systems, trustmark seals and complaint centers are used. [73]

Identity verification systems [73] use personal information about a customer in order to crosscheck that information against different databases to verify that the identity is correct.

Secure payment mechanisms [73] are different types of payments available to a customer. For example, eBay offers a variety of different ways to pay, and one of them is through PayPal. Each way of paying is supposed to ensure that no fraud is committed during the payment.

An escrow service [73] is an organization independent from the seller and the buyer. It takes the money and the goods, makes sure everything is correct before it delivers the money to the seller and the goods to the buyer. This is recommended by eBay to be used in payments above $500.
Feedback rating systems [73] are simple systems where the buyer rates a purchase from someone according to certain criterions and the different rates a seller gets are published on the auction website. The systems force the seller to behave well in order to get good rates, otherwise the seller will not be trusted and no one will buy anything from him/her.

Trustmark seals [73] are another way of rating sellers. Trustmark seals can be placed on sellers which have fulfilled certain criteria. A trustmark seal can for example be placed on somebody who has sold a lot of goods during a long time and has received a lot of positive feedback during that time. Trustmark seals pinpoint trusted sellers instead of rating everybody as feedback rating systems do.

Complaint centers [73] can be provided in order to let customers complain about a seller or buyer. The complaint centers can solve disputes among online customers.

To detect auction fraud certain programs are used [73]. The programs scan databases and screen users in order to find certain patterns which may indicate an ongoing fraud. eBay uses Fraud Automated Detection Engine (FADE) which detects fraud by screening and analyzing eBay's databases for fraud patterns and comparing the transactions with reported frauds.

### 7.2.3 Phishing countermeasures

There are some existing countermeasures against phishing. The ISP Earthlink [74] has a toolbar with a “scamblocker”. The “scamblocker” alerts the user before it enters a website which is on a list of known phishing sites. Spoofstick (from CoreStreet) [75] is a small browser extension which displays the real domain name of the displayed website in order to make it possible for the user to decide if it is a real or fake website. Symantec [76] provides a solution which blocks phishing mails by blocking e-mails with spoofed e-mail addresses and e-mails which contain spoofed URLs. Their solution also makes it possible for a user to be alerted when personal information is sent to a web site which not is on a list of trusted web sites managed by the user. E-commerce companies are also providing tools which tell their customers when they are on spoofed sites. eBay has a service in its toolbar called Account Guard [77] which alerts
their customers when they are on eBay’s or PayPal’s websites and when they are on websites known to spoof their web appearance.

There is e-mail software with embedded phishing protection on top of the ordinary spam-filter. SurfControl [78] has for example an URL-filter which scans incoming e-mails for URLs and compares them to a list of categorized websites in a database. The database is updated continuously and contains categories like phishing websites, adult websites etc. Another example is Eudora [79], which has a function called ScamWatch in their e-mail software. The function gives the user a warning whenever the user clicks on a link in an e-mail and if the link has a numerical IP-address, if the URL shown is different to the actual URL or if the domain name contains a top-level domain (for example www.fraud.liu.se.to).

Some ISPs block users from visiting fraudulent websites [77]. When for example a customer at AOL reports a spam, the website linked from that spam e-mail is blocked automatically for all of AOL’s customers.

Brands also try to monitor the use of their names [77]. This is done by monitoring both registrations and usages of similar domain names. Some also use web crawling technologies to monitor the use of the brand’s name on the Internet.

There are suggestions on different techniques which can be used to authenticate the sources of an e-mail [77]. The secure Internet messaging company Tumbleweed has a market-ready solution based on signatures using the S/MIME protocol. But also Yahoo and Microsoft have solutions which they want to implement in the future. Yahoo’s solution is called DomainKeys and Microsoft’s is called Caller-ID.

The Financial Services Technology Consortium (FSTC) has together with APWG (Anti Phishing Working Group) [80] proposed a project proposal for a project aiming at finding a long term solution for the phishing problem.
7.2.4 Spam countermeasures

A big problem in spam fighting is that people have different opinions about what is spam. Hence spam fighting systems should preferably be customizable by the user. [81]

Spam filters classify messages in order to give them a score and/or category to use as input to the filter part, which decides which e-mails to be considered as spam [81]. The classifying part analyzes the header, body and/or structure of the message. The classifying part may also consider one message at a time and/or compare the message to other ones. There are many different kinds of classifying mechanisms. One example of a filter is Chung-Kwei [82], developed at IBM Watson Research. This filter uses a pattern-discovery algorithm called Teiresias on a large amount of spam e-mails in order to find patterns, and then tries to find the corresponding patterns in new incoming e-mails to identify spam. Filtron [83] is a prototype of a filter based on statistical learning algorithms. The filter learns from examples of spam and ordinary e-mails in the user’s inbox. SpamBayes [84] is another filter which is using Bayesian networks to identify spam, the filter is trained with both ordinary e-mail and spam. There are also filters which try to recognize words or phrases in the e-mails [85], but a problem with those filters are that the spammer can change the words to some extent to make it understandable for a human, but not for the filter.

Another approach to fight spam is black lists and white lists [81]. These lists contains either e-mail addresses who are approved to send e-mail to your inbox (white lists) or e-mail addresses who are forbidden to send e-mails to your inbox (black lists). White lists are known to identify non spam e-mail very efficiently, but a problem is that the user must look through the e-mails from addresses that are not on the white-list in order to find non-spam e-mails from addresses not added to the white list. Black list are known to block innocent senders and sometimes domains inappropriately. In Goldbeck and Hendler’s [86] work they use a social network system based on reputation among the users in order to classify an e-mail address as good or bad. Cloudmark [87] uses a similar approach where every user can notify the community when a spam is received. The spam is then blocked for the other users in the community.
Another approach is to use honeypot e-mail addresses [81] that are non-active e-mail addresses which are used to identify spam. Since the addresses are non-active and are only spread on different websites on the Internet, every e-mail sent to these addresses is considered as spam. Symantec [88] has a system which uses this technique.

There are some suggestions of having payment systems for e-mail in order to increase the cost for a spammer [81]. But there are major political issues with payment systems. One suggestion is called “attention bonds”, where a user can set a price for which an unknown sender can send an e-mail. The price is paid as a bond. The bond is returned to the sender when the recipient acknowledges the e-mail as non-spam, otherwise the recipient keeps the bond as a payment for time wasted.

7.3 Addressing e-fraud challenges

In this section the challenges from Section 6.2.5 are considered one by one to see if they are addressed by the countermeasures in Section 7.1 and Section 7.2. High-level countermeasures against the challenges are also presented. The countermeasures presented here are not solutions to the problems, rather proposals for what a solution should do and thereby proposals for future work. Each subsection covers one challenge and starts by pointing out the existing countermeasures addressing the challenge and then presents some proposals for possible solutions. At the end of this section the proposed countermeasures are summarized.

7.3.1 Anonymity

Anonymity is only addressed by feedback systems and trustmark seals on auction websites which are used to let users share their opinion about a seller on an auction website, making it harder for the seller to hide the consequences of its actions.

One major reason that anonymity is not addressed to a larger extent even though it is a well-known problem is that it is a property of many services. E-mail providers do not for example demand that a user proves his/her identity when opening an e-mail account and do not want to do it either. To fight anonymity is to make it harder for
the fraudster to stay anonymous during proposal communication and committing. The basic idea of the existing countermeasure can be used to create solutions:

- **Provide feedback from other users.** Users’ actions can be shown and exposed to other users by publishing feedback from other users in order to show which users to trust. This is done on auctions websites, but can be done is several more domains, for example bulletin boards can rate users’ posts, and e-mail-addresses can be rated by the people receiving e-mails from it.

### 7.3.2 Automation

Automation in the sense of bots automatically performing actions is somewhat addressed by fraud detection systems (such as those in e-commerce and on auction websites) which may find patterns in bots’ behaviors and detect their activity. But the primary purpose of these systems is not to detect that programs are using the service. Reviews and organizational actions can protect against automatic frauds in business systems.

To fight automation is to stop the fraudster from committing and communicating proposals automatically using programs or similar. Since this is not a part of the web service normally, this should be made impossible. This can be done using the following countermeasures:

- **Make it impossible for programs to perform actions on web services.** In other words humans should be able to use the web service, but not a program.

- **Make it impossible for the fraudster to have more computers than his/her own working for him/her.** This is in order to limit the effects of automation when it occurs.

Another part of automation is that it makes it harder to detect fraud because points of detection are in the automatic part, this can be addressed by the following countermeasure:

- **Perform fraud detection on automatic systems.** Of course a consideration of what kind of frauds to look for is needed and the detection should be done using accurate techniques.
Manual reviews may also be considered in the detection to use the human “common sense”.

7.3.3 Available victims

The preventive measure of informing possible victims about risks and frauds which they are likely to be exposed to is one way of minimizing the number of available victims. Although it does not stop the fraudster from communicating proposals to the victims, it makes the victims more likely to utilize points of detection during the frauds. The different ways of addressing spam also address this problem. They do not minimize the number of victims, but it does make it harder for the fraudster to communicate during proposals. Some phishing countermeasures also limit the availability of victims by filtering and blocking of e-mail.

To fight available victims is equal to making it harder for the fraudster to communicate with a lot of persons during proposals and when sending information. The problem is that some people should be able to communicate to a lot of victims by using the same web services as the fraudster uses. There are however some solutions:

- **Provide feedback from other users.** Make web services where the senders are rated based on feedback from the recipients. If the fraudster reaches many possible victims in a service as this, the victims which recognize the fraudulent in the content of the message will use the possibility to grade the user to show other users that the message is not trustworthy.

- **Make it impossible for programs to perform actions on web services.** This makes it impossible for the fraudster to communicate automatically to a lot of victims and therefore has the fraudster perform more work on its own in order to reach all the available victims.

- **Teach users about frauds.** Teach possible victims about frauds in order to make them able to recognize when they are contacted by the fraudster. Both tools warning users for possible threats and information about frauds are possible solutions in this area.
7.3.4 Fraud cost

In one sense increases every countermeasure which makes it harder for the fraudster the cost for the fraud. But this category focuses mainly on the cheap costs for the fraudster of committing and communicating proposals in the e-fraud cases compared to the telecom cases. There are suggestions of introducing costs for e-mail, but these are not likely to go through. If they would, the price for communicating during proposals would rise for the fraudster.

As seen, this challenge is almost not addressed at all and since the cost for the non-fraudulent user should not be raised in web services, no solution to this challenge has been found.

7.3.5 Speed

Spam and phishing countermeasures can stop the speed of communication with a lot of people by making it harder to send fraudulent e-mails, thus taking longer time for the fraudster to communicate with each victim during the proposals.

In this challenge the speed of communicating and committing proposals are faster in the e-fraud cases compared to the telecom cases. This is a basic property when working with computers and Internet and no user wants an e-mail to take as long time to send as an ordinary mail. The speed of for a non-fraudulent user can therefore not be affected by the countermeasures against the speed for the fraudster. Even so, some countermeasures exist:

- **Make it impossible for programs to perform actions on web services.** This makes it impossible for the fraudster to utilize the speed of a program performing actions at a web service at much higher speed than possible by a human.

- **Make it impossible for the fraudster to have more computers than his/her own working for him/her.** This is in order to limit the amount of work that can be performed in parallel and thus raising the speed of the proposal communication or committing.
7.3.6 Ubiquity

This challenge is only partially addressed by fraud detection systems in e-commerce and on auction websites. They can to some extent detect if some user is acting as a crowd by comparing IP-numbers, looking at behavior etc thus utilizing points of detection.

In order to find countermeasures against ubiquity is it important to notice that acting as several users is not fraudulent itself. An ordinary user can have several e-mail addresses. There are some countermeasures which can help anyway:

- **Make it possible to identify when a single user has several usernames.** This is not an easy task and it does not solve the problem itself, but it is an important feature to use in order to point at possible fraudulent behavior.

- **Make it possible to identify the same user in different services.** This helps in finding patterns of fraudulent usage if a lot of users are using both of the services to perform a task, like for example eBay and PayPal. But it demands that the services are interconnected and share information about the users.

- **Make it possible to connect users to geographical positions.** Even though this can not be used in order to detect fraud, someone can for example order things from USA to his/her relatives in Japan while working in Germany. This can be used to highlight suspicious transfers which should be further investigated. The scenario from the example is after all not that common.

- **Make it impossible for the fraudster to have more computers than his/her own working for him/her.** This is in order to be sure that computers (IP-numbers) can be connected with persons in order to simplify the implementation of the three points above and also in order to stop the fraudster from acting as a crowd in terms of computers.

7.3.7 Lack of interconnection

This challenge can not be addressed by countermeasures mentioned in Section 7.1 and Section 7.2. Instead, it needs to be addressed by
cooperation between different owners of different web services and websites in order to share information from the different services in order to make it possible to utilize different points of detection. An interconnection of all the services is impossible since the organization handling that interconnection would be too “big brother”-like to be publicly accepted. The only possible solution for a web service to address this problem is to find other web services which are used in conjunction with the web service and cooperate with them in order to find fraudsters.

7.3.8 Novel users

In e-commerce third-party guarantees as World-Pay and Fia-Net make sure the merchant is trustworthy for a novel user which can not make that judgment alone. On auction websites escrow services have a similar role. Both guarantee that no fraud will be conducted during the proposal from the possible victim’s point of view. In phishing several tools are offered in order to warn novel users when they are being exposed to a fraud. Toolbars in browsers control each visited website against an updated list of spoofed websites, or by displaying the domain name separately in order to avoid URL-spoofing. This helps the novel users to identify points of detection and utilize them, without having the knowledge needed to do it on their own. Information of all kind helps also novel users to see signs of frauds and to discover points of detection by themselves.

Novel users will always exist to greater or lesser extent, since everyone is a novel user at the beginning. It is never realistic to make the assumption that there are no novel users. There are however some tool which may be used in order to help novel users to discover the points of detection which they should discover in order to avoid fraud:

- **Provide feedback from other users.** By providing feedback on both services and users, more experienced users can share their experience with novel users and show that a service or a user can or can not be trusted. Then, as the novel user’s experience grows, former novel users can judge users and services that have not been rated yet.
• **Develop tools which warn users and points at points of detection for different frauds.** This is in order to help novel users to find points of detection and also in order to teach them about them. This can involve everything from highlighting an e-mail address when it is formerly not known to the user to pointing out domain names of websites.

• **Teach users about frauds.** Teach novel users in order to make them experienced users as fast as possible. The natural way to do this is to show information about different frauds as much as possible and spreading news about new frauds as they occur.

### 7.3.9 Summary of proposed countermeasures

The following countermeasures have been proposed in this section:

1. Make it impossible for programs to perform actions on web services.
2. Provide feedback from other users.
3. Make it impossible for the fraudster to have more computers than his/her own working for him/her.
4. Make it possible to identify when a single user have several usernames.
5. Make it possible to identify the same user in different services.
6. Make it possible to connect users to geographical locations.
7. Develop tools which warn users and points at points of detection for different frauds.
8. Perform fraud detection on automatic systems.
9. Teach users about frauds.

The order of the list describes the priority to implement and deploy these countermeasures. It is important to notice that some implemented versions of these countermeasures exist (e.g. feedback systems). But even so, these counter measures need to be investigated further in order to see where they can be used and if the implemented countermeasures provide the needed functionality.

### 7.4 Discussion

In this section the need for standards and the proposed solutions about making it impossible for programs to perform actions on web
services and providing feedback from other users are discussed in order to show some interesting points within these subjects.

7.4.1 The need for standards

It is important to stress that some countermeasures may not have the desired effect if they do not become standards. For example, a fraudster is likely to use stolen credit card details at a website which do not use 3-D Secure. Hence different systems should become (after careful consideration) standards in order to remove old systems which are easier for a fraudster to attack.

7.4.2 Consequences of proposed solutions

The countermeasure of making it impossible for programs to access web services includes several interesting consequences. The countermeasure makes it impossible for the fraudster to implement a fraud automatically, which is possible now. At present date a fraudster can figure out a fraud schema, and even if a single iteration of the fraud schema makes a little profit, the possibility of letting a program make all iterations makes it possible for the fraudster to make a big profit. Moreover, this countermeasure makes it harder for spammers to get e-mail addresses to use for spam, since this is often carried out by programs. Finally, it simply slows down the fraudster, since the fraudster must do everything in same pace as the normal user.

Providing feedback from other users has been proven to be abused and manipulated. Systems implementing this type of countermeasure must take in consideration that friends will support friends (even the fraudster’s friends) and user names with high rating can be bought and sold etc. There is also a possibility for fraudsters to perform some simple action in order to get a higher ranking and then perform the fraud having the high ranking. But even if there are problems, even simple systems make it harder for the fraudster to fool victims.
8 Conclusions

This chapter presents the major conclusions in this thesis.

8.1 Answering problem description

These are the answers to the main problems from the problem description in Section 1.2.

1. How do instances of e-fraud currently look like?

In Chapters 4 and 5 detailed answers are given to this problems. The most important general conclusions are presented here.

E-frauds are currently widely spread on the Internet and there are several different schemas within several sophisticated techniques are used in order to achieve the fraud’s goal. There is a big economic loss each year because of e-frauds.

There is often a repetitive part in the e-frauds and for each repetition of this part does the fraudster gain profit. This repetitive part can in some cases be used to mount up small profits of each repetition to a large total profit. The small profits are hard to detect in fraud detection systems. Cases where both the fraudster and the victim are private persons are also considered as simple, making them easy to detect if the knowledge to detect them exist. Many cases can be detected by investigating the content and origin of received messages, but some cases can be detected by investigating user behaviors or by detecting that a program is communicating with the web service.

2 Are there real-world fraud schemas which do not exist on the Internet and are likely to transpose to the Internet?

Since no real world fraud classification systems or taxonomies offers the properties required for classifying all kinds of fraud in a non ambiguous way, is it not possible to use any of them to predict frauds in new environments, such as Internet. Combining the existing classification systems or taxonomies is not considered as an option, since the diversity of the goals pursued by each methodology.
Instead have telecom cases studies been compared to e-fraud case studies finding that the concepts from the telecom cases are already existing in the e-fraud cases. But this conclusion can not be made for all real world frauds, since there are no proofs that there are no other concepts in other fraud domains in the real world. Telecom cases are however believed to represent a majority of the concepts, since frauds have a long history in the telecom environment.

3 What are the differences between e-fraud and real world-fraud cases?

Out of a comparison between e-fraud and telecom fraud cases studies has the following challenges with e-fraud prevention and detection been found:

- Anonymity
- Automation
- Available victims
- Fraud cost
- Speed
- Ubiquity
- Lack of interconnection
- Novel users

But the following possibilities with e-fraud prevention and detection has also been found:

- Interpretation
- Available data

These differences are extracted from a comparison between e-frauds and telecom frauds, but are they considered as representative differences between e-frauds and real-world frauds. The major consequence of the challenges is that e-fraud cases are more scalable in both finding and dealing with victims.

4 What countermeasures are needed to fight e-fraud?

There are many countermeasures which address specific e-frauds, such as phishing and auction fraud. There are also countermeasures which address techniques used in e-frauds, such as spam. But the countermeasures considered in this thesis have been proven to
address the challenges in e-fraud prevention and detection in very small extent. Therefore proposes this thesis the following high-level countermeasures in order to address the challenges:

- Make it impossible for programs to perform actions on web services.
- Make it impossible for fraudsters to use other computers than its own working for itself.
- Provide feedback from other users.
- Make it possible to identify when a single user have several usernames.
- Make it possible to identify the same user in different services.
- Make it possible to connect users to geographical locations.
- Develop tools which warn users and points at points of detection for different frauds.
- Perform fraud detection on automatic systems.
- Teach users about frauds.

8.2 Future work

This thesis have found no reason to continue the work of investigating if there are real-world frauds which are likely to transpose to the Internet, both because telecom frauds are already conceptually transposed to the Internet and because of the extent of e-fraud today.

Instead is it more interesting to investigate concrete solutions to the high level countermeasures presented in this thesis. Each single one of these countermeasures is a proposal for further work in order to develop new countermeasures against e-fraud.
References


[46] Byers S. A. D. Rubin and D. Kormann, “Defending against an Internet-based attack on the physical world”, ACM


[56] Painter C. M. E. “Tracing in Internet Fraud Cases: PairGain and NEI Webworld”, Bulletin, U.S. Department of Justice, April 16, 2003. Also available online at


Appendix A – Telecom fraud case analysis

Case 1 – An old fraud

The protocol model for case 1:

The function model for case 1:

Values:
x: The bet on the horse
y: The result from the bet on the horse (either 0 or win)

Functions:
y = F(x) - The money transferred to the fraudster is a function of the bet
Case 2 – Subscription fraud

The protocol model for case 2:

The function model for case 2:

Values
x: The calls the fraudster makes and the telephone the fraudster gets
y: The bill the fraudster is suppose to pay

Functions:
y = F(x) - The amount on the fraudsters bill is dependent on the calls made by the fraudster
Case 3 – 809 telephone scams

The protocol model for case 3:

Proposals:
1: Call this number and get information about your brother
2: Proposal for paying the bills for the calls

The function model for case 3:

Values:
x: The fraudsters information which is reached through the PRS-number
y: The PRS income from Linda's calls

Functions:
y = F(x) - The amount the company gets is related to the amount of information Linda gets from the company
Case 4 – Prepaid fraud

The protocol model for case 4:

The function model for case 4:

Values:
\( x \): Money used to buy the voucher numbers
\( y \): The account is recharged

Functions:
\( y = F(x) \) - The amount recharged is depending on the amount of money used to buy the voucher numbers
Case 5 – Premium rate services fraud

The protocol model for case 5:

The function model for case 5:

Values:
- \(x\): The service presented by the PRS number
- \(y\): The amount paid for the PRS number calls
- \(z\): The value given to the company hosting the PRS service for the income on the calls to the PRS service

Functions:
- \(y = F(x)\) - The amount paid for the PRS service depends on how much you have used the service
- \(z = F'(x)\) - The amount paid to the company depends on how much people have used the service
Case 6 – Cloning fraud

The protocol model for case 6:

The function model for case 6:

Values:
x: The calls made abroad
y: The amount paid according to the roaming agreement
z: The bill for the calls made from abroad

Functions:
y = F(x) - The amount paid according to roaming agreement is depending on the calls made
z = F(y) - The amount of the bill is depending on the amount paid in the roaming agreement
Case 7 – PBX fraud

The protocol model for case 7:

The function model for case 7:

Values:
- \( x \): The calls made by the company
- \( x' \): The calls made by Thelma’s customers
- \( y \): The money Thelma’s customer pay Thelma
- \( z \): The money Naive Inc. pays National Telecom for their telephone bill

Functions:
- \( y = F(x') \) - The amount paid depending on the calls made by Thelma’s customers
- \( z = F(x + x') \) - The amount of the bill is depending on the calls made by the company and Thelma’s customers
Case 8 – Internet Modem Switch Scam

The protocol model for case 8:

The function model for case 8:

Values:
- \( x \): Access to the porn site
- \( y \): The PRS income from Morgan's modem's calls

Functions:
\[ y = F(x) \] - The amount the porn site gets is related to the time Morgan uses the PRS number

88
Appendix B – E-fraud case analysis

Case 1 – Nigerian letter fraud

The protocol model for case 1:

![Diagram of protocol model]

The function model for case 1:

![Diagram of function model]

Values:
- x: Money to pay fees
- y: Money left on Stephen’s account

Functions:
- \( y = F(x) \) - The amount Stephen gets depends on the fees paid
Case 2 – Financial fraud

The protocol model for case 2:

Proposals
1. Proposal for buying stocks for a certain amount of money
2. Proposal for buying stocks for a certain amount of money
3. Proposal for selling stocks for a certain amount of money

The function model for case 2:

Values
x: Money to buy stocks
z: Money to buy stocks
y: Money for selling stocks
t: Money for selling stocks

Functions:
y = F(x + z) - The amount received when selling the stocks depends on the amount bought, the amount bought by other buyers and the development on the stock market
t = F(z) - The amount received when selling the stocks depends on the amount bought and the development on the stock market
Case 3 – Money laundering

The protocol model for case 3:

Proposals:
1: Transfer money from PayPal to the account
2: Play poker with these credits
3: Transfer money from the account to a bank

The function model for case 3:

Values:
x: Money to account
y: Money after gambling

Functions:
y = F(x) - The money returned depends on the result in the gambling
Case 4 – Internet auction fraud

The protocol model for case 4:

The function model for case 4:

Values:
- x: Payment for the goods
- y: The goods

Functions:
- \( y = F(x) \) - The goods sent depends on the money paid
Case 5 – Business to business fraud

The protocol model for case 5:

The function model for case 5:

Values:
x: Payment for the goods
y: The goods
z: Payment for the goods
t: The goods

Functions:
y = F(x) - The goods sent depends on the money paid
z = F'(t) - The goods sent depends on the money paid (Overcharging)
Case 6 – Triangulation

The protocol model for case 6:

The function model for case 6:

Variables:

- x: Payment for a computer
- y: Payment for a computer
- z: Payment for goods
- a: Repayment for fraudulent transactions
- b: Repayment for fraudulent transactions

Functions:

- f(x) = - The computer sent depends on the paid money
- f(y) = - The amount needed depends on the computer
- f(z) = - The goods sent depends on the paid money
- f(a) = - The money paid to Virginia depends on the amount in the fraudulent transactions
- f(b) = - The money paid depends on the amount paid to Virginia

Proposals:
1. Proposal for buying a computer
2. Proposal for buying a computer made by a program
3. Proposal for buying goods made by a program or a person
4. Demanding of money back for fraudulent transactions
5. Demanding of money back for fraudulent transactions
Case 7 – Phishing

The protocol model for case 7:

The function model for case 7:

Values
x: Payment for goods
y: Goods
z: Repayment for fraudulent transactions
i: Repayment for fraudulent transactions

Functions
y = F(x) - The goods sent depends on the money provided
z = F(x) - The money paid to John depends on the amount in the fraudulent transaction
i = F(z) - The money paid depends on the amount paid to John
Case 8 – Extortion

The protocol model for case 8:

Proposals:
1: Pay $40,000 or get hit by a DoS-attack
2: Pay $50,000 or get hit by a DoS-attack

The function model for case 8:

Values:
x: Money paid for avoiding attack
y: Income from players

Functions:
y = F(x) - The income depends on the amount of money paid to the fraudster
Case 9 – Automatic bidding

The protocol model for case 9:

The function model for case 9:
På svenska

Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extraordinära omständigheter uppstår.

Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art.

Upphovsmannens ideella rätt innefattar rätt att bli nämnd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se förlagets hemsida http://www.ep.liu.se/

In English

The publishers will keep this document online on the Internet - or its possible replacement - for a considerable time from the date of publication baring exceptional circumstances.

The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: http://www.ep.liu.se/

© Bengt Bergman