FIDIS

Future of Identity in the Information Society

Title:	D5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research
Author:	WP5
Editors:	Ronald Leenes (Tilburg University, The Netherlands)
Reviewers:	Peter Sommer (London School of Economics, UK)
	Jozef Vyskoč (VaF, s.r.o. Slovak Republic)
Identifier:	D5.2b
Type:	Deliverable
Version:	1.0
Date:	Friday, 05 May 2006
Status:	[Final]
Class:	[Public]
File:	fidis-wp5-del5.2b.ID-related.crime.doc

Summary

This deliverable contains the consolidated version of the papers that were prepared for the ID fraud Workshop, held on 18 May 2005 in Tilburg, the Netherlands. The papers discuss ID-related crimes from a legal, a socio-economic, and a technical perspective. It provides an initial presentation of the vast array of phenomena commonly addressed as ID fraud or ID theft from the various perspectives. The legal chapter briefly discusses the EU legal framework as well as some of the national ID crime provisions. The socio-economic chapter decomposes ID linkage into ID collision, ID change, ID deletion and ID restoration in order to gain a more detailed understanding of the various types of ID crimes. It also discusses the incidence of ID crimes as well as the social and economic effects for victims and businesses. The technical chapter describes a number of technical methods of ID crime, including different perspectives on biometrics. Finally, a chapter on countermeasures describes various socio-economic and technical measures to combat ID-related crime.

The objective of this deliverable is to start creating a common ground on which further interdisciplinary research on ID crimes can be developed. The chapters are separate building blocks, put together as a first step to develop such a common ground.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1.	***Goethe University Frankfurt***	Germany
2.	***Joint Research Centre (JRC)(IPTS)***	Spain
3.	***Vrije Universiteit Brussel***	Belgium
4.	***Unabhängiges Landeszentrum für Datenschutz (ICPP)***	Germany
5.	***Institut Europeen D'Administration Des Affaires (INSEAD)***	France
6.	***University of Reading***	United Kingdom
7.	***Katholieke Universiteit Leuven (COSIC)***	Belgium
8.	***Tilburg University (TILT)***	Netherlands
9.	***Karlstads University***	Sweden
10.	***Technische Universität Berlin***	Germany
11.	***Technische Universität Dresden***	Germany
12.	***Albert-Ludwig-University Freiburg***	Germany
13.	***Masarykova universita v Brne***	Czech Republic
14.	***VaF Bratislava***	Slovakia
15.	***London School of Economics and Political Science***	United Kingdom
16.	***Budapest University of Technology and Economics (ISTRI)***	Hungary
17.	***IBM Research GmbH***	Switzerland
18.	***Institut de recherche criminelle de la Gendarmerie Nationale***	France
19.	***Netherlands Forensic Institute (NFI)***	Netherlands
20.	***Virtual Identity and Privacy Research Center***	Switzerland
21.	***Europäisches Microsoft Innovations Center GmbH***	Germany
22.	***Institute of Communication and Computer Systems (ICCS)***	Greece
23.	***AXSionics AG***	Switzerland
24.	***SIRRIX AG Security Technologies***	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	18.05.2005	Initial working papers: • Ronald Leenes - legal • Svetla Nikova - technical, • Ioannis Maghiros, Sabine Delaitre - socio-economic
0.2	02.08.2005	• revised socio-economic paper (Sabine Delaitre, Martin Meints)
0.3	24.09.2005	• initial integration (Martin Meints, Ronald Leenes)
0.4	24.09.2005	• major text revision (Ronald Leenes)
0.5	02.10.2005	• Included improvements made by ICPP to the social chapter (Ronald Leenes, Martin Meints)
0.6	02.10.2005	• draft (Ronald Leenes)
0.7	23.02.2006	• draft review version (Ronald Leenes)
0.8	02.03.2006	• review version (Ronald Leenes, Bert-Jaap Koops)
1.0	05.05.2006	• final version (Ronald Leenes)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 Executive summary	Ronald Leenes (TILT), various chapter authors
2 Introduction	Ronald Leenes
3 Legal aspects	Ronald Leenes, Hans Graux (ICRI)
4 Socio-Economic aspects	Martin Meints (ICPP), Martin Rost (ICPP), Albin Zuccato (KAU), Sabine Delaitre (IPTS), Ioannis Maghiros (IPTS)
5 Technical aspects	Svetla Nikova (COSIC), Sebastian Clauß (TUD), Vicky Andronikou (ICCS), Klaus Kursawe (COSIC), Zeno Geradts (NFI)
6 Countermeasures	Svetla Nikova, Sebastian Clauß, Vicky Andronikou, Klaus Kursawe, Zeno Geradts
7 Conclusions and further work	Bert-Jaap Koops (TILT), Ronald Leenes

Table of Contents

1 Executive Summary 8

2 Introduction 10

2.1 ID-related crime: a preliminary definition 10
2.2 eCommerce related ID crime: when business opportunities go awry 15
2.3 Techniques and practices: the tools of the trade 18
2.3.1 phishing 19
2.3.2 sniffing 22

3 Legal Aspects 25

3.1 ID fraud from a legal point of view 26
3.1.1 The European legal framework 27
3.1.2 ID fraud decomposed 30
3.2 Some cases and legal responses 37
3.2.1 eBanking and white hat hacking: ID crime with a twist 38
3.2.2 e-mail ID fraud and gambling 39
3.2.3 Legal frictions? 40
3.3 Conclusion 41

4 Social and Economic Aspects 42

4.1 Introduction 42
4.2 Identity Change, Identity Fraud and Identity Theft from a sociological point of view 43
4.3 Establishing persons as entities in social systems 43
4.3.1 General properties with respect to rearrangement of identity linkage 48
4.4 Towards a typology of rearrangements of identity linkage 50
4.4.1 Identity collision – definition and types 50
4.4.2 Identity change – definition and types 51
4.4.3 Identity deletion 54
4.4.4 Identity restoration 55
4.5 "Identity Fraud" 55
4.5.1 “Identity fraud” in social systems 57
4.5.2 General theses on the appearance of "identity fraud" 59
4.5.3 The transition from identity collision to "identity fraud" 60
4.6 Incidence of Identity Theft and Identity Fraud in Society 61
4.6.1 Corporate Identity Theft and Fraud 65
4.7 Social and Economic Aspects 66
4.7.1 Social Aspects 67
4.7.2 Economic Aspects 69
4.8 Conclusion 77

5 Technical Aspects 78

5.1 Introduction 78
5.1.1 Authentication of a person by an IT system 79
5.1.2 Authentication of an IT System by a Person 82

5.1.3 Methods to manipulate Authentication Procedures 83
5.2 Two scenarios for identity fraud with biometrics 85
5.2.1 Scenario 1: Attacking an authentication, identification and tracking system using physical biometrics 86
5.2.2 Scenario 2: Possibilities of Identity theft with biometric devices 89
5.2.3 Conclusion 93

6 Countermeasures 95

6.1 Social and technical guidelines on preventing ID-related crimes 96
6.1.1 Socio-economic guidelines 96
6.1.2 Technological guidelines 97
6.1.3 Digital identities 99
6.2 Authentication technologies 101
6.2.1 Biometrics 102
6.2.2 Identity management 106
6.2.3 Trusted Platform Module 107
6.3 Conclusion 107

7 Conclusions and further work 107

7.1 Towards talking about the same thing 107
7.1.1 Terminology 107
7.1.2 Conceptual framework 107
7.1.3 Definitions 107
7.2 Towards combating the same thing 107
7.2.1 Legal measures 107
7.2.2 Social-economic measures 107
7.2.3 Technical measures 107
7.2.4 The right mix of measures 107

8 References 107

9 Annex 107

9.1 Index of Tables 107
9.2 Index of Figures 107

1 Executive Summary

Identity fraud appears to be on the rise. The phenomenon is spreading from the USA, where ID theft already is one of the most frequent crimes, to Europe. ID theft seems to have a relatively clear meaning. However, when one scratches a little below the surface, the concept is less clear. The current deliverable provides an overview of some of the difficulties surrounding the area of Identity-Related Crimes. This work is based on three papers prepared for the FIDIS WP5 ID Fraud workshop, which was held on the 18th of May 2005 in Tilburg, the Netherlands. The three papers discussed identity-related crimes from three distinct perspectives: a legal, socio-economic, and technical one. The current document provides a consolidation of the three papers.

The workshop and this document show that our understanding of ID theft and ID fraud is still limited. For instance, in everyday language we speak about ID theft. In many jurisdictions this term is imprecise from a legal perspective as the identity of the victim is not stolen – like one can steal a car –, but copied. The original identity bearer does not lose her identity by the act of 'ID theft'. This may seem trivial, but in criminal law, the phrasing of criminal provisions is essential. This example suggests that we need to refine our concepts and define a proper ontology of the relevant phenomena. This document aims to be a starting point for this work. It elicits relevant distinctions in the field and provides for a common ground on which follow-up research can be founded.

Chapter two delineates the field by defining a working definition that highlights essential features:

> 'ID fraud is when someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non-existing person.' (Grijpink, 2003)

This chapter furthermore shows that identity crime usually consists of a sequence of steps, starting with fishing for the identity data, the misappropriation, misuse of the data and finally, a criminal act. Part of the sequence, the fishing and misappropriation stages, are illustrated by means of two common techniques, phishing and sniffing.

Chapter three discusses the legal aspects of identity crimes. It shows that, with the exception of the USA, identity theft and identity fraud as such are not criminal offences in most jurisdictions. Instead there is a patchwork of legal provisions, both on the European level as well as on the national level within the EU member states that cover some of the specific forms of identity crimes. These can be related to the sequence discussed in chapter two. The criminal action, for instance covers crimes such as the acquisition of financial benefits without right. The discussion on the types of identity-related crimes shows that there are differences between the EU jurisdictions that warrant further research in order to provide advice on harmonisation.

Chapter four provides an analysis of the types of identity mix-up. This results in four basic categories:

1. identity collision
2. identity change
3. identity deletion
4. identity restoration

Identity change can be further decomposed into four sub-types:

a) identity takeover

b) identity exchange

c) identity delegation

d) identity creation

The four types of identity change introduced can all be legal or illegal. The illegal subset of identity change is generally called "identity fraud", but a better term would be "criminally motivated identity change".

Chapter four also discusses some of the statistics on Identity crimes. This shows that reliable statistics are lacking and that there is a potentially large dark number. This is partly due to the fact that identity crimes (ID theft, for instance) are breeder offences which usually lead to other criminal activity. Hence, it is difficult to demarcate the costs and incidence. The impact of identity crime on individuals and companies is discussed. Furthermore the reasons why identity crimes are difficult to tackle are touched and potential measures and incentives for businesses to improve security are discussed.

Chapter five approaches identity crimes from a technical perspective by analyzing the entities, both human and machines, involved. It discusses some examples of techniques that can be deployed by perpetrators, for instance, attacks on authentication in a (shopping mall) surveillance scenario, to show that also traditional settings enhanced by technology are prone to identity misuse. The final section of this chapter addresses ways to misuse biometrics, which shows that this relatively new technology on which high hopes are vested can also be misused.

Chapter six presents a number of socio-cultural and technical countermeasures against identity crime. In the former category we find measures such as increasing risk awareness and reconsidering authentication needs. The technical guidelines focus on ways to improve authentication and digital identities. It also discusses the role of biometrics to improve authentication. Finally, the trusted computer platform is discussed as a means to enhance security in IDM systems.

Chapter seven draws some conclusions and provides an agenda for further research.

2 Introduction

This document presents the results of a WP5/WP8 workshop on ID theft and ID fraud held on 18 May 2005 in Tilburg, the Netherlands. For this workshop three papers were written from different perspectives on ID theft and ID fraud: socio-economic, legal, and technical. The present document provides an integration and consolidation of these three papers. The workshop and this document show that our understanding of ID theft and ID fraud in the 'online world'[1] is still limited. For instance, while common parlance denotes the topic of this work to be ID theft, this term is imprecise from a legal perspective as the ID is not stolen – like one can steal a car – but copied. The original identity bearer does not lose her identity by the act of 'ID theft'. This suggests that we need to refine our concepts and define a proper ontology of the relevant phenomena. This document is more limited in scope, though. It aims to offer a first analysis of the components, from a legal, social and technical perspective, that together comprise 'ID-related crimes' as we will denote the range of misuses of ID numbers and other data. The next chapters will provide classifications of phenomena and methods based on applying the different perspectives.

The authors are aware that further development and integration should take place in order to advance our understanding of this relatively new, and rapidly growing, set of phenomena associated with the rise of the information society.

The present chapter provides a first sketch of ID-related crimes and provides some examples of ID crimes and the legal responses to these crimes. It also discusses the two common forms of these crimes from a more technical point of view: phishing and sniffing.

2.1 ID-related crime: a preliminary definition

ID theft has entered the mainstream media judging from the fact that major newspapers have had specials on ID theft and regularly report about major incidences of large scale ID misappropriation. Also, magazines, such as Newsweek have featured cover stories on ID theft.

Generally these reports describe some of the horror stories resulting from, for instance, the fact that a victim has lost identifying data (e.g. credit card) as a result of some internet scam. The culprit typically uses the data (name, credit card number and expiry date of the card) to buy goods thereby rapidly depleting the victim's credit limit. The stories then continue to

[1] The work in this deliverable relates primarily to ID related crimes committed in the 'online world'. By this imprecise term we mean that the focus is on behaviour on the Internet, or in any case involving electronic means. The forgery of paper documents by means of the artful copying by a con artist falls outside the scope of this deliverable, whereas copying the data on an RFID tag in a biometric passport is included. We acknowledge that the border between what is intended to be included and what not is not always clear. Stimulating discussion on the border is one of the objectives of this deliverable/

depict the obstacles the victim has to take in order to remediate the wrongs inflicted by the culprit. Finally words of caution and tips on ID fraud prevention are given.

Often, these accounts lack a clear definition of ID theft and ID fraud. Although crimes relating to Identity and ID papers are not new – even before medieval times people impersonated others by taking on false identities[2] – defining ID-related crimes in the online world is not completely without problems.

In this section we discuss some of the difficulties in delineating ID theft and ID fraud.

Terms such as ID fraud, ID theft, and ID-related crime are used interchangeably, and are often taken to be synonyms. There are, subtle, differences and one of the objectives of the current chapter is to clarify the confusion with respect to the various terms.

A common term for ID-related crime in the EU is ID fraud. In a study by the UK Cabinet Office (2002, p. 9), this is described as:

> 'ID fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent.'

Jan Grijpink in the Netherlands uses a slightly broader definition. Identity fraud means

> 'that someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non-existing person' (Grijpink, 2003).

In comparison to the former definition, not only the name, but also other identity tokens, such as facial resemblance, fingerprints, or other data can be used to put the recipient on the wrong foot. The notion of identity is not further specified in this definition, nor in many of the other ones. Elaborating on the nature of identity is necessary as will be discussed in chapter 4. An act that many would include in the list of ID fraud is pretending to be a representative of an organisation, such as the Social Security department, or the electricity board, in order to persuade people to pay for some kind of service. Hence, not only taking someone's civil identity comprises ID fraud, but also the illegitimate assumption of an organisational role. Also note that Grijpink does not address consent, or the lack thereof, of the 'victim'. Lacking in both definitions so far is the notion of context. Is someone who wears a (rented) police uniform during carnival committing ID fraud? Probably we would not go this far. However, if the same person on his way home confiscates someone's car, it would be a case of ID fraud. In Grijpink's definition the latter would comprise malicious intent, whereas this is absent in the former case.

Apart from these general definitions, there are also domain-specific definitions. For instance, the Dutch Ministry of Justice uses the following definition:

---

[2] See http://www.caslon.com/idtheftprofile1.htm for an illuminating overview.

> 'Identity fraud concerns forms of misuse or fraud with respect to identity and identity data, with which a person or a group of persons intends to unlawfully claim government services [Dutch: overheidsprestaties], or to otherwise unlawfully benefit himself'.[3]

Another common term for identity related misuses is ID theft. Mitchison et al. in their JRC discussion paper on Identity Theft state:

> 'Identity theft, in what in this paper is called its 'paradigm' form, occurs when one person – in this study a "rogue" – obtains data or documents belonging to another - the victim - and then passes himself off as the victim (Mitchison, et al., 2004).'[4]

In the same line, we find specialised forms of ID theft, such as the one described by Michael Perl:

> 'Criminal record identity theft occurs when the identity thief obtains a victim's personal information and then commits crimes, traffic violations, or other illegal activities while acting as the victim. Instead of providing law enforcement with her own personal information, the identity thief provides the victim's personal information in order for the identity thief to avoid criminal convictions and legal sanctions in her own name.' (Perl, 2003)

The US Identity Theft and Assumption Deterrence Act[5], one of the few statutes that contain provisions directly sanctioning identity theft, defines ID theft *inter alia*, as

> 'the knowing transfer or use, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.'

The ID theft and ID fraud definitions may seem to overlap sufficiently to warrant using them as synonyms at first sight. The also seem to be universally applicable. From a legal perspective this is not the case. The principle of legality which underlies most penal law systems requires crimes and misdemeanors to be formulated precisely to warrant legal certainty. Hence, the definition (or conditions for applicability) of ID-related misuse matters.

In the Netherlands, for instance, theft relates to tangible 'goods' according to article 310 of the Dutch Penal Code. The Dutch High Court has ruled that an essential characteristic of 'goods'

---

[3] Dutch Ministry of Justice, 'Hoofdlijnen kabinetsbeleid fraudebestrijding 2003-2007, 24 June 2003 [translation Bert-Jaap Koops].

[4] Interestingly, lending my bank card to my spouse and asking her to get me some money from a cash machine whilst I stay in bed with the flu, would according to this definition be identity theft. We will discuss this matter in more detail in section 4.4.

[5] Section 1028 (a)(7) of title 18 of United States Code sanctions.

is that the possessor necessarily loses possession of the good as a result of the theft. Information, or data in general, can not be stolen by the act of copying: the owner still has his/her copy of the data.[6] This implies that one's (digital) identity can not be stolen. Identity papers can be stolen, but using someone else's username and password, or using credit card data is not theft. And hence 'ID theft' is in effect an improper term for this kind of misconduct. The term ID fraud does not suffer from this problem, and would therefore in the Netherlands be the preferred term.

Theft also suffers from another problem. Since theft is a term from the penal domain, it hides the fact that ID fraud also, or maybe more so, belongs in the civil law domain. Using someone's identity may result in Tort as the victim is likely to suffer damages as a result of the use of her identity without this person's consent. This is another reason to use the term ID fraud (or 'Identity crime') instead of ID theft.

We will return to this issue in chapter seven which summarises the analysis of ID-related crime from the different perspectives and presents plans for further research.

For now, we will use Grijpink's definition as it highlights a number of features that we deem essential for the phenomenon we are interested in:

> ID fraud is when someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non-existing person.

The features of interest are:

- malicious intent: this means the rogue has to act with the intent of committing criminal actions (after taking on the identity of the victim);
- consciously: the rogue has to intentionally (knowingly) take on the 'false' identity;
- create a semblance: any form that tricks a third party in believing that the rogue is indeed the victim is included;
- another one's identity: the use of one's own identity is not ID fraud;
- using: only actual use, not merely possession, of the acquired identity is what constitutes fraud.
- existing or non-existing: identities of both living and dead, existing or fictitious identities can be used.[7]

---

6 HR 3 December 1996, NJ 1997, 574.

7 This includes al four types of identity change discussed in chapter 4: identity takeover, identity exchange, identity delegation, identity creation.

This definition also shows that ID fraud in itself usually is not the aim of the action. The perpetrator takes, or creates another one's identity with the aim of using this identity for other, illegal or otherwise malicious, actions. So irrespective, whether ID fraud in itself is a criminal offence, which as we will see later is not the case in many jurisdictions, this definition emphasises a chain of events associated with typical ID fraud. Such a chain of events typically looks like figure 1 (Mitchinson *et al*, 2004).

Fishing for data is the step in which the perpetrator is looking for data to be used for the false identity. In the online world this may include actions such as phishing (see section 2.3.1)

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Figure 1. ID fraud sequence, taken from Mitchison (2004, p. 21)

Misappropriation concerns getting hold of the actual identification data, be it a document or just information (such as a social security number (SSN)). This stage corresponds to what the UK Home Office calls Identity Theft: when sufficient information about an identity is obtained to facilitate Identity Fraud.[8]

By **misuse** the Mitchinson *et al* means that the false identity is established, but has not been used for any illegal action.

And finally, the **criminal action** is the stage in which the false identity is used for some illegal action, such as credit card fraud, or benefit or tax fraud. This stage corresponds to the UK Home Office's definition of Identity Fraud: 'when a False Identity or someone else's

[8] http://www.identitytheft.org.uk/definition.html

identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Fraud'.[9]

The sequence makes clear that the misappropriation, the act that best resembles the concept of 'stealing' the identity, is not the end, nor the beginning.

Taking the other stages into account and also looking at the various reasons for acquiring another person's identity is necessary to understand the nature of ID-related crimes, from a legal perspective, both also from the other perspectives adopted in this report.

Reasons for appropriating another person's identity, the reason for misuse in other words, can be found in three areas according to the UK Cabinet Office's ID fraud study (2002, p.9):

- To avoid being identified in the original identity (concealment);

  This includes illegal immigrants, people with poor credit histories trying to obtain financial services, but also people working under cover, including law enforcement officers.

- To make financial profit from some form of fraud;

  In the private sector this reason includes credit card misuse while typical uses in the public sector include obtaining welfare benefits.

- To avoid financial liability.

  Here a range of activities such as Tax avoidance, reneging outstanding debts and avoiding paying child benefit are prime examples.

We should now have sufficient background to look at ID-related crimes in somewhat more detail.

2.2 eCommerce related ID crime: when business opportunities go awry

Given the reasons for assuming other people's identity, it should not come as a surprise that in the online world Electronic Commerce (eCommerce from now on), and up to now to a lesser extent eGovernment[10], are obvious areas where ID-related crimes flourish. eCommerce is a phenomenon that is almost as difficult to describe as ID crime itself. Defined at its broadest (any form of business activity that is completed partially or in whole using telecommunications), it is as old as the notion of telecommunications itself. In a more strict sense, the notion refers solely to business transactions that have been concluded through the

---

9 http://www.identitytheft.org.uk/definition.html

10 This probably relates to the fact that eGovernment is less advanced and has fewer users than eCommerce as of yet.

Internet or a similar network.[11] It is in this sense that the expression is most commonly used nowadays, and this is also the interpretation of the notion that we use in this chapter.

The rising prevalence of ID crime is inextricably linked to the increase acceptance of eCommerce by everyday consumers. Indeed, the main selling point of eCommerce is and always has been the possibility of new business opportunities. eCommerce achieved its major breakthrough in the late nineties, when all involved parties began to realise this potential. For businesses, it was obvious that eCommerce offered the potential of reaching new markets, thus increasing user bases, revenue and (hopefully) profit. For consumers, the potential lay in the expected increase in competition, which could lower prices, improve service and offer more choices. However, as with any other form of social interaction, eCommerce also offered the possibility of abuse. The availability of personal information led to an increase in ID-related crimes, as privacy sensitive information suddenly became more vulnerable and more valuable than ever before.

A woman in Liège, Belgium discovered the truth of this assessment in February 2000, when her phone and e-mail were all of a sudden overrun with rather explicit romantic proposals from complete strangers. A brief investigation revealed that her vindictive ex-boyfriend decided after their painful break-up to assume her identity and express an interest in amorous adventures on an on-line dating forum, using a message that included her number and e-mail address. Suffice it to say that the culprit was quickly arrested, and soon thereafter convicted[12] for forgery and stalking[13]. Although the facts themselves are trivial enough, this decision is still interesting from a legal perspective, as the penalisation of neither crime (forgery or stalking) was specifically drafted with the internet or ID crimes in mind. In fact, the Belgian Penal code specifically requires the use of a writing (nl: *geschrift;* fr: *écriture*) in order for a given set of facts to qualify as a forgery. Nonetheless, the judge in this case decided to interpret this requirement in a flexible manner, and decided that assuming another one's identity in an on-line forum without their consent could constitute forgery[14]. Thus, existing

---

[11] Examples of more formal definitions abound, see e.g. http://help.econ.census.gov/econhelp/glossary/ : "E-commerce (or electronic commerce) is any business transaction whose price or essential terms were negotiated over an on-line system such as an Internet, Extranet, Electronic Data Interchange network, or electronic mail system. It does not include transactions negotiated via facsimile machine or switched telephone network, or payments made on-line for transactions whose terms were negotiated off-line."

[12] Corr. Luik, 18 november 2002, Ubiquité, 2003, p.95, noot O. LEROUX.

[13] In the official terms of the law: *valsheid in geschriften / faux en écriture* (article 193 of the Penal Code) and *belaging / harcèlement* (article 442bis of the Penal Code).

[14] This is particularly interesting to note, because several months after the facts, the ICT Crime Act of November 28 2000 was approved in Belgium, introducing a new crime into the Penal code by the name of ICT forgery (*valsheid in informatica / faux en informatique*). This new provision was precisely intended to resolve the debate regarding the applicability of traditional qualifications such as forgery in an on-line context. However, since the facts described above predated the new legislation, this qualification could not have been withheld by the judge, who resorted instead to a more extensive interpretation of existing laws.

general legislation was considered to be sufficient as a framework for sanctioning this instance of ID theft.

Of course, this particular case was fairly trivial, having neither large financial consequences for its victim, nor any real benefit for the perpetrator (other than, perhaps, a fleeting sense of satisfaction). However, the ease with which an alternate identity could be assumed in a social context is already indicative for the potential damage that ID crime can have. Besides its obvious boons, eCommerce offers the possibility of a fairly low risk crime, where low investments can potentially yield larger gains than more traditional forms of fraud. We shall take a closer look at these more serious crimes and their financial impact below.

That the prevalence of ID crimes is increasing is a fairly generally accepted fact, as indicated above. However, the size of this increase (or indeed, the prevalence and magnitude of the crimes themselves) are to a very large extent unknown. The two most major problems in accurately assessing the size of the problem lies both in the definition of ID-related crime and in the large dark number. The result is that statistics underestimate the prevalence and can not be compared on an international level.

As a quick indication, the US Federal Trade Commission claimed in February 2005 that ID fraud now *affects* 10 million Americans each year, and *had a dollar volume* of 52,6 billion dollars in 2004 (roughly 40,3 billion €)15. The exact meaning of both numbers is not explained. By way of comparison, a recent Gartner US survey stated that more than 1.4 million people have been victims of identity fraud, costing banks and credit card issuers $1.2 billion in 2003 in new account, checking account and credit-card fraud (Litan, 2004). Even keeping into account the difference in terminology, the discrepancy between both figures adequately demonstrates the lack of reliable metrics in this field.

As mentioned above, this increase in ID crime is a natural consequence of the increasing cash flow in eCommerce. This, in turn, is a consequence of consumers' growing confidence in electronic payment transactions. To a large extent, this newfound confidence is not purely the result of natural market trends (i.e. consumers slowly becoming aware of the potential advantages of on-line transactions), but also of deliberate attempts to stimulate this new form of business. On a European scale, this becomes evident with only a passing glance at the eCommerce legal framework. As early as 1997, the European Commission declared the promotion of a favourable (e)Business environment to be a top priority, stating that the creation of consumer awareness and confidence was an essential part of such an environment.[16] Additionally, a series of directives[17] was passed that were intended specifically

---

[15] See http://www.ftc.gov/opa/2005/02/ncpw05.htm

[16] Commission communication of 18 April 1997: A European Initiative in the sector of Electronic Commerce, COM(97) 0157, not yet published in the Official Journal

to achieve this goal of consumer confidence, by granting consumers an unprecedented level of protection in on-line transactions.18 One can only conclude that encouraging on-line transactions has (rightly) received a great deal of European attention. However, it appears that the same attention has not been given to protection against on-line ID crime.

This is unfortunate, as this means that consumers are less likely to be informed of on-line risks than of on-line benefits (the second condition mentioned in the introduction), possibly resulting in a false sense of security. As consumers become increasingly aware of the relative safety of electronic payments (both in an on-line and off-line context) criminal opportunities are augmented, and successful fraud schemes become largely a matter of acquiring and efficiently manipulating personal data.

One of the sectors that has been forced to become aware of this problem quite rapidly is eBanking. The reasons for this are apparent: users of eBanking are, by definition, at ease with sending important personal information over a network; and their data potentially allows access to larger sums of money, since damages in the case of eBanking ID theft are not necessarily limited to a single transaction. As such, eBanking is a model target for ID criminals, offering large rewards for a relatively small effort.

2.3 Techniques and practices: the tools of the trade

In this section we focus on eBanking as a particularly striking example for eCommerce's vulnerability to ID crime. We will take a closer look at several common techniques for ID crime (most of which are also in common use for other forms of eCommerce crime), along with a few real-life cases and the legal response to it. We will specifically examine the interesting cases of phishing (a more recent phenomenon whose popularity has soared in the last two years) and sniffing (a common activity for network traffic analysis that is unfortunately quite prone to abuse by ID criminals). The relatively common case of hacking will not be examined as it is not specifically tailored towards ID crime and therefore falls outside of the scope of this deliverable.

For the purposes of this section, we define eBanking as the use of telecommunication (specifically the Internet) for the purposes of managing bank accounts, investments, portfolio's and such, including the electronic completion of transactions. Typical examples of

---

[17] Such as the Distance Sale Directive and the Distance Contracts for Financial Services Directive (respectively: European Parliament and Council Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts (Official Journal L 144 of June 4th 1997); and Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC (Official Journal L 271 of October 10th 2002).

[18] Including e.g. a temporary risk-free right of withdrawal; a right of reimbursal in case of payment card fraud; and protection against so-called inertia selling.

eBanking services include banking websites and payment software. In the present context, we are of course mostly concerned with the use of eBanking tools by consumers, as this is where the greatest ID crime risk lies.

2.3.1 phishing

Phishing (simply pronounced "fishing", in fine hacker tradition[19]) is a fairly new term for a technique that is becoming increasingly common for aspiring ID criminals. The core concept of phishing is simple and effective, based on common methods of social engineering: victims are approached in a manner that superficially seems trustworthy, and are simply asked to hand over sensitive data. The etymology of the expression is immediately clear: perpetrators are metaphorically "fishing" for data the victim is willing to hand over.

As such, phishing has a longstanding offline tradition. The easiest way to gain access to confidential information is not to steal it, but to simply ask for it. With a small amount of social manipulation (e.g. presenting one's self as part of the IT maintenance department) a surprisingly large number of victims appears to throw all caution in the wind. The reason why phishing has recently garnered so much attention is because of a new trend: combining phishing with mass e-mail sending (similar to spamming activities), and relying on the pure size of the victim base to ensure a good return on this scam.

A simple example: assuming that a scammer sends out one million e-mails per day, and has a reply rate of 1%, and only 1% of those replies yields useful information, then the result is still 100 willing victims. Merely using the information to shift €100 from their bank accounts means a daily return of €10.000. Some of these numbers may seem high at first sight, but consider that top spammers have been shown to send out up to 10 million e-mails on peak days, and claim a reply rate between 3 and 5 %, and suddenly the estimate appears a great deal more modest. It should come as no surprise that Tower Group research estimated phishing damages to amount to 120 million € in 2004, and rising rapidly. Considering the dark number problem, criminal profits in this type of crime are nothing short of staggering.

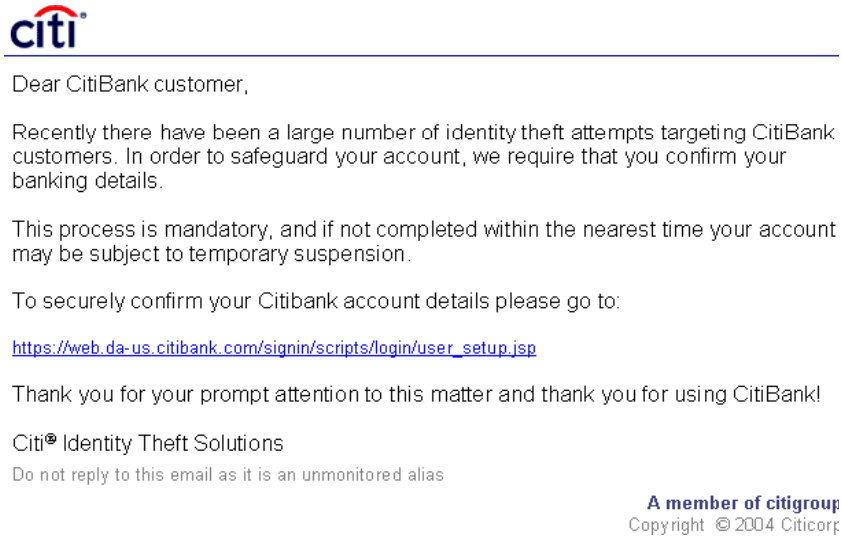
Financial institutions are obviously particularly attractive targets for this type of scam[20], as the requested information permits the direct transfer of funds to an account abroad. To make the

---

[19] Its most famous predecessor is, of course, *phreaking* (again pronounced as "freaking"). This specific activity, mostly popular in the seventies and eighties, involved using a modem to send a specific sound signal over a phone line, thus falsely suggesting to the phone center that the phone was being used by internal maintenance crew. The desired result was obviously a free phone call. A more recent example is "pharming", the intentional corruption of local DNS caches, so that even the introduction of a perfectly correct web-address (such as www.ebay.com) could lead to a hacked website without the visitor's knowledge.

[20] The December 2004 Phishing Activity Trends report from the Anti-Phishing Working Group indicates that approximately 85 % of all phishing mails attempt to present themselves as originating from the financial services sector. Other common feigned origins were ISPs (7%) and retail (6%). See

scam mails particularly believable, they typically rely on emulating existing and reputable brand names to the greatest possible extent.[21] As an example, we will take a closer look at a typical recent[22] phishing e-mail, pretending to be originating from Citibank. It appeared as shown in figure 2.


citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

Copyright © 2004 Citicorp

Figure 2. Phishing example impersonating CitiBank.

The e-mail uses the following tricks to mask its intent:

- Abuse of the Citibank logo and trademark to establish or promote trust.
- Warning of dangers of identity theft, thus appearing to have good intentions. It also prompts the user to act quickly, as his account may otherwise be temporarily suspended.
- A warning not to reply to the e-mail "as it is an unmonitored alias"; in reality the reason is of course that the sender's e-mail address was spoofed and would result in an error, thus giving the scam away.
- The entire text was included in a graphic file, rather than as actual text. In this way, the scam could not easily be detected by software filters that only rely on text analysis.
- The indicated link was obviously also part of the image file; in fact, clicking anywhere on the text (i.e. the graphic file) would have resulted in the victim visiting the forged website, where he would be asked for his bank account credentials.

---

http://antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20December%202004.pdf

[21] The December 2004 Phishing Activity Trends report (mentioned above) indicated that only six or seven brand names are used in 80% of all phishing e-mails, Citibank being the prime target.

[22] The author received this mail in October 2004

- The link itself led to a site that was hosted on a private user's computer, who was in all likelihood unaware that his system was being abused for this purpose[23]. This method offers greater anonymity for the scammer, whose system is never directly connected to his victims[24].
- If the mail had only contained the graphic file, certain software filters might still identify it as a scam mail. For this reason, it contained one line of randomly generated text in a white colour. This text was invisible to any human reader (as it was displayed on a white background), but it would have been perfectly legible to a software filter.

From a European perspective, this type of scam violates a number of regulations[25], such as:

- A number of offences in the European Council's Cybercrime convention, such as illegal access (when a third party's system is hacked to display the phishing site), computer-related forgery (the actual e-mail itself) and computer-related fraud (by using the stolen data to assume the victim's identity).[26]
- The data protection directives[27], to the extent that harvesting and abusing the victim's personal data constitutes illegal processing.
- Intellectual property regulations, to the extent that the name or trademark of an unrelated organisation is abused for criminal purposes. On a European scale these

---

[23] This is a common modus operandi, and this is also the reason why scam websites still enjoy a fairly long uptime: they are unknowingly hosted by private users, rather than on a professional ISP's systems. The December 2004 Phishing Activity Trends report (mentioned above) indicates that an average scam site remains online for no less than 5.9 days; the largest measured online time was 30 days.

[24] This system is also one of the reasons that potential victims often receives almost identical scam mails several times in a short period of time: when one hacked site goes down, another system is hacked, and an updated mail is sent to the same potential victims. By way of example, the author has received 40 nearly identical phishing mails in a period of two weeks (between February 7th and February 14th 2005). This repetition also increases the social pressure on potential victims to reply by suggesting a sense of urgency. Although it does obviously beg a simple question: why do scammers believe that a ruse that has consistently failed 39 times in a row will suddenly work on the 40th try?

[25] The regulatory framework will be discussed in chapter three.

[26] At the European Union level, the proposal for a Council Framework Decision on attacks against information systems has roughly the same aims. As a result, phishing would also violate the corresponding offences in this proposal, most notably the provisions related to illegal access (COM(2002) 173 final - Official Journal C 203 E of August 27th 2002)

[27] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281 of November 23rd 1995; and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Official Journal L 201 of 31 July 2002).

problems are governed by a number of regulations including the Berne Convention[28] and the directive on Copyright in the information society.[29]

Obviously, phishing will also violate national transpositions and related regulations in the national law systems of the Member States.

2.3.2 sniffing

Sniffing is a general IT-term related to the analysis of network traffic. Using a "sniffer" program, all or part of the network traffic passing through a given node of that network is captured for later analysis. As an example, the author ran a network analysis program[30] while logging on to the internal FIDIS website (http://internal.fidis.net). One of the http-packets intercepted contained (among more technical data) the following information (Figure 3):

Source:	10.33.xxx.xxx	(the author's IP address, last two blocks masked)
Destination:	80.237.xxx.xxx	(The FIDIS site IP address, last two blocks masked)

Additionally, the HTTP packet contained 74 bytes of data, which decoded as:
"user=HGraux&pass=xxxxxx&submit=Login&logintype=login&pid=2&redirect_url="
(string decoded from its hexadecimal form, password has been masked)

Figure 3. Sniffing example.

As shown above, the intercepted package contained both the author's IP address, his FIDIS username and his password (for obvious reasons masked in the text above). Although the example provided is fairly innocent, it is clear that a small, hidden sniffer could be extremely useful for an aspiring identity thief.[31]

Similar to the phishing example above, using sniffing software as a tool for ID crime is in clear violation of a number of European regulations, including:

- a number of offences in the European Council's Cybercrime convention, such as illegal interception (of the data transmitted by the victim's computer) and computer-related fraud (by using the stolen data to assume the victim's identity).

---

28 See http://www.wipo.int/treaties/en/ip/berne/

29 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Official Journal L 167 of June 22nd 2001).

30 The software used was Ethereal; see www.ethereal.com

31 For eBanking purposes, sniffers will likely prove less effective, as financial services sites typically use extensive security precautions, including the SSL-protocol. In these cases, sniffing would only have yielded encoded data that would not be instantly useable.

- the data protection directives[32], to the extent that harvesting and abusing the victim's personal data constitutes illegal processing.

Again, sniffing will also violate national transpositions and related regulations in the national law systems of the Member States.

Sniffing presents one other interesting aspect that demonstrates that this activity is fundamentally different from phishing: sniffing has demonstrable beneficial uses. In fact, the pejorative connotation of the terminology is somewhat confusing. Sniffing is really nothing more than a slang term for network monitoring, which in itself is an essential aspect of computer network management. Indeed, system administrators rely on network monitoring software to trace network activity, locate bottlenecks and monitor network functionality (not necessarily by monitoring an individual user's activities).

As such, network monitoring software (or sniffers, depending on one's personal preference) is one of many applications that walk a fine line: even when designed for benevolent and perfectly legal purposes, it is very easy to abuse to achieve criminal goals. Regulation of such software remains a thorny issue to this day, as legislators struggle to find adequate criteria that would render sniffers illegal, yet permit network monitoring software. As indicated above, we believe that the difference between sniffing and network monitoring is largely semantic, and that any attempts to restrict the production and use of this software can have only a marginal practical impact.

This has not stopped regulators from trying, though. On a European level, e.g. the Cybercrime Convention forbids even the production[33] of "a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5 [...] with intent that it be used for the purpose of [such offences]." Its flaws are obvious: the production of such software is only illegal if the programmer had the *intention* of using it for criminal purposes, and if (s)he has *primarily* designed the software for this purpose. Both criteria are highly subjective, and will only allow the elimination of the clearest cases of abuse.

From a conceptual point of view, one may raise the question why specific tools should be outlawed, in addition to certain undesirable behaviours. Shouldn't a ban of criminal behaviour itself suffice without targeting the manufacturing of certain tools, when those tools can only

---

[32] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281 of November 23rd 1995; and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Official Journal L 201 of 31 July 2002).

[33] Article 6, 1, a) of the Convention. The possession of such software is also rendered illegal under similar conditions in article 6, 1, b).

rarely be shown to be intended for illegal purposes? The question is of a legal-philosophical nature, and falls outside of the scope of this paper. Nonetheless, it is worth bearing in mind.

3 Legal Aspects

In this chapter, we provide a first analysis of the legal framework with respect to ID misuse, or ID-related crime in the online world. We will focus on the EU framework, as provided by the various E-society directives, as well as look closer to national legislation in some of the EU member states. We will draw examples of ID misuse from commercial transactions. The potential value of successfully offering e-services and selling goods online is huge and the market grows as it partially replaces the offline market. The value of identification data in online interactions is increasing rapidly, as is the potential to do damage when this data is abused.

The potential for damage is further increased by the fact that generally electronic identification techniques are not secure, so that identity fraud is technically not too challenging for potential criminals; and a basic understanding of security techniques by average users is lacking, so that they are unaware of security risks and potential pitfalls. For example, the relative insecurity of e-mail (which has no reliable authentication mechanism integrated in its core functionality) means that an e-mail recipient can never be certain that an e-mail actually originated from the indicated sender. This basic requirement can only be met by using additional techniques, like digital signing, which also increases the complexity of e-mail communication somewhat. The lack of general public acceptance of these security techniques means that the average person still uses unauthenticated e-mail, which is a great facilitator to identity fraud in e-mail traffic.

Another factor is the lack of user awareness of the risks of on-line transactions. For example, many eBanking clients promptly provide their login and password whenever requested to do so in a mail message appearing to stem from the bank. Such a message should trigger caution, as there is no reason for their bank to ask for their user data as this data originates from the bank and is therefore already stored in their databases. Only when users subsequently find their accounts severely depleted several days later do they raise an eyebrow.

Also the legal framework leaves things to be desired. For instance, the phishing for data as described in the previous chapter is not a crime in many jurisdictions. It may be punishable under all sorts of legal provisions, but there is a relatively large amount of uncertainty if the behaviour is indeed punishable, and if so under which provisions.

The conditions outlined are, to a large extent, factors of time: eventually, more secure techniques will find their way to the general public, and more users will know better than to send important data to strangers and lacunae in legislation will be fixed. But in the mean time, it is interesting to see what practical problems exist, and what effect the actions of our legislators (both on a European and on a national level) are having. This is the question that this chapter tries to resolve: are current identity crime policies effective, and could the actual situation be improved by modifying the legal framework?

3.1 ID fraud from a legal point of view

In the previous chapter we have provided a brief analysis of ID-related misuse and we have looked at two areas in which these misuses come to light. In this section we explore the legal side of ID misuse in the on-line world.

As we have seen in figure 1, the process associated with ID-related crime can be broken down into four steps: fishing for data, misappropriation, misuse, and criminal action. Each of these steps can be covered by legal provisions. So, the phishing for data, its appropriation, misuse as well as the crimes committed with the acquired identity could all be subject to their own provisions in legislation. For instance, under the US Anti-phishing act 2005, which was introduced by Senator Patrick Leahy on 28 February 2005, phishing would become a crime under Chapter 63 of title 18, United States Code:

> Sec. 1351. Internet fraud
>
> (a) Website- Whoever knowingly, with the intent to carry on any activity which would be a Federal or State crime of fraud or identity theft--
>
> (1) creates or procures the creation of a website or domain name that represents itself as a legitimate on-line business, without the authority or approval of the registered owner of the actual website or domain name of the legitimate on-line business; and
>
> (2) uses that website or domain name to induce, request, ask, or solicit any person to transmit, submit, or provide any means of identification to another;

The broadest provision, and in fact the only one (or one of the only ones) that covers stages one to three[34], is the already mentioned US Identity Theft and Assumption Deterrence Act[35]. It addresses ID theft, as the knowing transfer or use, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

From the ID law survey that is being compiled as part of FIDIS work package 5, we may conclude that this in fact is the only provision in the countries studied so far that covers ID fraud as such.[36] As we have seen in the preceding sections, also the entry of computer systems that contain personal data (hacking) and the consequential modification of these systems for criminal purposes are used as criminal offences related to ID fraud. Another focus appears to be stage four: the crimes that can be committed using the false identity, such as tax evasion, or credit card fraud. Also from the side of the victim there are relevant legal provisions, as

---

[34] Or at least stages two and three.

[35] Section 1028 (a)(7) of title 18 of United States Code sanctions.

[36] The ID law survey can be found on http://rechten.uvt.nl/idls

storing and using the victim's identity can be a breach of the victim's privacy. Hence, data protection legislation may be relevant.

We will start our exploration with the European legal provisions relevant to our area of study.

3.1.1 The European legal framework

As EU Directives, as well as the Council of Europe Convention on Cybercrime play an important part in European jurisdictions, it is useful to take a closer look at the Directives relating to ID-related crime, as well as the Cybercrime treaty.

Unlike the US provision on ID theft, neither EU Directives, nor the Cybercrime treaty explicitly contain ID theft or ID fraud provisions. Rather, most relevant regulation is either focused on privacy protection in general, or on ICT crime in general. Identity theft and identity fraud, being at the crossroads of these two subject matters, will usually be covered by both, as the examples below will show.

The Privacy Directives

Where electronic transactions are concerned, the core of the European privacy protection framework consists of two directives:

- Directive 95/46/EC of the European Parliament of and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (commonly referred to as the "Privacy directive").[37]
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "Directive on privacy and electronic communications").[38]

Examining these directives in any detail would take us too far (especially considering their relative complexity). Suffice to say at this point is that they both concern the protection of personal data (defined as any information relating to an identified or identifiable natural person), and seek to protect the privacy of European citizens by determining the circumstances under which such data may be lawfully collected and processed. While the first directive treats this subject in the most general sense, the second directive focuses on privacy protection in the field of electronic communication (e.g. the protection of traffic data).

To show the relevance of these Directives and their transposition into national legislation, we can point at the provisions that regulate processing of personal data, which includes Identity data. In general data may be processed only under the following circumstances (Directive 95/46/EC, art. 7):

---

[37] Published in the Official Journal L 281, 23 November 1995, p. 0031-0050

[38] Published in the Official Journal L 201, 31 July 2002, p. 0037-0047

- when the data subject has given his consent;
- when the processing is necessary for the performance of or the entering into a contract;
- when processing is necessary for compliance with a legal obligation;
- when processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

The particular relevance of these directives lies in the fact that fraudulent collection and use of personal data (e.g. by intercepting personal communications and subsequently using another person's captured login data) will typically be a violation of these directives and their transpositions, as the data subject (the victim) will generally not have given her consent, not will any of the other requirements have been met.[39] An interesting issue is whether a victim of phishing can be said to have consented to the acquisition of their personal data.

But even if the subject can be said to have consented tot the acquisition of the personal data, then still the processing of these data will generally not be in accordance with the directive, as article 6b states that personal data can only be processed for specified, explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes.[40] We can be fairly certain that the phisher will not reveal the purpose of the phishing expedition, and hence the consent would not include agreement to the phisher's hidden motives. Possibly also the purposes will be illegal, which would inhibit the legitimacy of the data collection even further.

As the Member States are required to impose sanctions on this sort of conduct in their national data protection legislation, some forms of identity fraud will, at a minimum, be punishable as a violation of the privacy directives.

---

[39] Interestingly, EU member states can have slight variations and exceptions to the requirements for legitimate processing. The Slovak Protection of personal data Act, for instance, states explicitly that the law does not apply when personal data is acquired by accident, or when no intent to process the data in a systematic way exists. These conditions are exceptions to the consent requirement. {source: Jozef Vyskoč's review comments}

[40] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Council of Europe's Cybercrime Treaty

The Cybercrime Treaty is presently the most influential European text regarding cybercrime.[41] Since its adoption on 23 November 2001, it has been signed by 32 nations, including a number of non-European states such as Japan, Canada and the USA. Its most significant contribution is the introduction of a number of harmonizing provisions, both in substantial and procedural criminal law. Although the Treaty only entered into force as recently as 1 July 2004, Member States have been aligning their legislations to its provisions since its inception, so that its provisions can be considered indicative for general European cyber crime legislation.

As with the Privacy directives, the provisions of the Cybercrime Treaty do not specifically address identity crime as such. They do, however, define a number of crimes that are typically committed in conjunction with identity crimes, such as:

- article 2 - illegal access: intentionally accessing a computer system without right, e.g. by hacking into a computer system with the intention of stealing personal data from it
- article 3 - illegal interception: intentionally intercepting without right, made by technical means, of non-public computer transmissions of computer data. E.g. monitoring internet traffic in the hopes of capturing login names or passwords.
- article 7 - computer-related forgery: intentionally introducing, altering or deleting data in a computer system without right and with the intent that is be considered or acted upon for legal purposes as if it were authentic, e.g. by introducing a false password into an eBanking system and transferring the victim's funds to another account
- article 8 - computer-related fraud: intentionally and without right, causing of a loss of property to another person by;
    - any input, alteration, deletion or suppression of computer data,
    - any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

These provisions may apply to stages two to four of the sequence outlined previously, even though they were not specifically drafted for this purpose. As the treaty is not binding to citizens and states have to transpose these provisions in national law, the scope of the resulting provisions can either include or exclude ID-related crimes.

It is worth noting that a similar, more limited instrument has been taken in the European Union. The Council Framework Decision of 24 February 2005 on attacks against information systems[42] has a similar objective as the Cybercrime Treaty, although its scope is more limited by targeting a number of crimes against computer systems ("information systems"), such as illegal access and illegal interference, which could also be used to combat identity crime.

---

[41] See http://conventions.coe.int

[42] Council Framework Decision 2005/222/JHA, *Official Journal* 16 March 2005, L69/67.

3.1.2 ID fraud decomposed

The discussion of the European legal framework shows that no specific ID crime related provisions exist at this level. This has prompted us to study various jurisdictions with respect to ID-related crimes in more detail. This study is part of the ID law survey that is carried out in FIDIS workpackage five (WP5). At present only a limited number of countries have been studied, and even here the depth of the analysis is insufficient to pretend to have a clear overview. What the analysis so far reveals, however, is that there are no specific ID theft provisions in at least, Belgium, France, Greece, Italy, the Netherlands, Slovakia, Spain, and the UK. The US, as mentioned, has specific provisions, both on a Federal level, as well as in various states.

Specific provisions to address types of ID fraud and ID theft may not be necessary as the actions involved may already encompass criminal actions under current legislation. And in fact, as sections 3.2.1 and 3.2.2 will illustrate, this may be sufficient to cope with the relatively new forms of ID fraud. The ID law survey tries to gain insight in the way the various jurisdictions handle ID-related crimes. The initial typology used in the survey showed the following distribution across the various jurisdictions.

	BE	FR	GR	IT	NL	SK	ES	UK	USA	FI	DE
ID theft	-	-	-	-	-	-	-	-	√		
ID fraud			-		-		-		√*	-	
ID doc fraud					√		√				√
immigration document fraud									√		
paper fraud		√			√					√	
computer fraud		√					√		√		
mail fraud									√		
wire fraud									√		
financial institution fraud		√							√		
internet fraud									√		
ID document forgery	√	√			√	√	√		√		√
forgery	√	√			√		√		√	√	
unlawful data collection	√	√			√		√				√
unlawful data use		√					√				
ID doc damage						√	√				√
imposture	√	√			√				√	√	

Table 1. ID Law Survey summary (as of May 2005)[43]

The taxonomy currently used for the survey is less fine grained than depicted in Table 1. ID Law Survey summary (as of May 2005) and consists of the following types:

1. ID-specific crimes
2. Fraud
3. Forgery
4. Damage
5. Data Abuse
6. Imposture
7. Tort
8. Personality rights

[43] The * means that there are multiple provisions, both on the federal level as well as on the level of the states. A '-' means there are certainly no specific provisions, a √ means there are specific provisions. An empty cell means that no positive or negative information is available yet. The greyed bars relate to the area covered by the Privacy Directive. Some countries have more detailed provisions than the more general ones in the Directive.

The detailed analysis of these types of crimes in various (European) jurisdictions goes well beyond the scope of this deliverable, but in order to give a flavour of what such a comparative study entails we will discuss some of these items in somewhat more detail, drawing from the WP5 ID law survey, Mitchison *et al* and other sources.

1 ID-specific crimes

This category includes specific criminalisation of ID theft, ID fraud, or ID document crimes (e.g., fraud, forgery, theft, damage, trade, receiving of official ID document or of unofficial ID document).

As discussed earlier, the 'taking' of a person's identity may or may not comprise theft. In the Netherlands (and Belgium) at least, the crime of theft relates to tangible goods ('things'), of which can be said that the owner loses control over it when it is stolen. This includes electricity as electricity can only be used once. Entities that may have multiple incarnations can not be stolen. Information (such as a PIN code[44]) and computer data which can be copied without undermining the owner's capabilities of use (multiple use), can therefore not be stolen. Unauthorised copying of computer software is an offence under the Copyright law, though[45].

In the UK, the story with respect to theft is different. The central provision here is the UK Theft Act 1968, which states (in 1-(1)) "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it ; and 'thief' and 'steal' shall be constructed accordingly". Property includes, according to 4-(1) of the same act 'money and all other property[46], real or personal including things in action and other intangible property.' This is much broader than property under the Dutch regime as it includes intangible property without defining what this encompasses. But in a sense it is also stricter as tangibles such as 'wild mushrooms, fruits or foliage on wild plants' are excludes, as is land (4-(2) and 4(3)). What is stolen has to belong to another, meaning that the person ('owner') has possession or control of it, or has any proprietary right or interest.[47] Appropriation according to section 3 of the 1968 Ac means: any assumption by a person of the rights of an owner. The thief has to have the intention of permanently depriving the other of it, which excludes lending as a criminal offence, unless the period and circumstances make it equivalent to an outright taking or

---

44 Dutch High Court (HR 13 June 1995, NJ 1995, 635).

45 E.g. Article 45h Auteurswet 1912

46 How we love these circular definitions in law.

47 UK Theft Act 1968 5-(1).

disposal.[48] According to the UK Crown Prosecution Service[49], tampering with electricity supply is not theft, since electricity is not property. This offence is addressed in section 13 of the 1968 Act.

Given the discussion on the Dutch and Belgian provisions, we are, on the basis of only looking at the provision and not at relevant case law inclined, to conclude that as no deprivation occurs when ID data is copied, theft does not entail ID theft under section 1 of the UK Theft Act 1968. Yet, mention is made of the possibility to prosecute ID theft under section 1 of the act, but only when the perpetrator made a monetary gain.[50] Case law should provide an answer to the question whether section 1 of the 1968 Act offers any resort to fight Identity Crime. The UK Home Office Identity Fraud Steering Committee in any case is investigating whether specific provisions are required.

Depending on purpose and type of information acquired other provisions in the 1968 act may apply as discussed under the next heading.

In other jurisdictions these distinctions with respect to what is, and what is not, subject to the action of theft may be absent.

2 Fraud

Mitchison et al (2004), when discussing fraud write: "*Fraud* is the crime of intentional use of deceit, a trick or other dishonest means to deprive another of his money, property or a legal right. Inherent in fraud is an unjust advantage over another which injures that person or entity.[51]

Information fraud – provided for as a specific crime in some legal systems[52] - mainly consists in the illegal enrichment through the illegal use of an information system (such as the alteration of data or software) (Mitchison et al., 2004)."

Fraud generally is defined in a technology neutral form, and hence many countries have fraud provisions that can be used in the battle against ID Fraud. Finland, for instance, in chapter 36 of the penal code, section 1 (1), defines a fraudster as 'a person who, in order to obtain unlawful financial benefit for himself/herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person…'. Similarly, the German Criminal Code in section 263

---

48 UK Theft Act 1968 6-(1).

49 Http://www.cps.gov.uk/legal/section8/

50 Http://www.computeractive.co.uk/computing/features/2072420/identity-theft-protect-survive

51 See http://dictionary.law.com

52 See http://dictionary.law.com

defines Fraud as '(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts,…'. Sweden

More detailed provisions are also available. The UK Theft Act 1968 as amendend in 1996 in section 15a (1), Obtaining a money transfer by deception, declares 'A person is guilty of an offence if by any deception he dishonestly obtains a money transfer for himself or another.' In all cases the financial gain of the perpetrator is an essential element of the provision.

Yet, here also, we are subject to the intricacies of national jurisdictions. Drawing again on the Netherlands and Belgium, as these are the countries the authors are most familiar with, we see clear differences.

The Belgian Penal code has two relevant provisions: article 496 which cover virtually any form of fraud where a person attempts to entice others to hand over any form of property (vermogensvoordeel), through the use of false names or assumed functions, or other forms of deceit (e.g., by suggesting the existence of a fictitious enterprise). In 2000, section IIIbis was added, containing a separate article 504quater on IT fraud (informaticabedrog), defined as "the fraudulent acquisition of a property advantage for himself or for another, through the introduction, alteration, deletion or modification of the possible use of data which is stored, processed or transferred by means of an information system through any technological means".[53]

In the Netherlands, article 236 of the Dutch Penal Code[54] provides a provision that clearly resembles the Belgian one. However, there is a subtle difference that makes the provision

---

[53] In Dutch: Art. 496. Hij die, met het oogmerk om zich een zaak toe te eigenen die aan een ander toebehoort, zich gelden, roerende goederen, verbintenissen, kwijtingen, schuldbevrijdingen doet afgeven of leveren, hetzij door het gebruik maken van valse namen of valse hoedanigheden, hetzij door het aanwenden van listige kunstgrepen om te doen geloven aan het bestaan van valse ondernemingen, van een denkbeeldige macht of van een denkbeeldig krediet, om een goede afloop, een ongeval of enige andere hersenschimmige gebeurtenis te doen verwachten of te doen vrezen of om op andere wijze misbruik te maken van het vertrouwen of van de lichtgelovigheid, wordt gestraft met gevangenisstraf van een maand tot vijf jaar en met geldboete van zesentwintig frank tot drieduizend frank.
Art. 504quater. § 1. Hij die, voor zichzelf of voor een ander, een bedrieglijk vermogensvoordeel verwerft, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

[54] Article 326 Dutch Penal Code: Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige

totally unsuitable to address acts such as phishing. The provision requires the object that is taken (defrauded) from its owner to represent a value in legitimate trade. As there is no legitimate market for credit card data, user names, password etc, the act of phishing does not classify as fraud under said provision.

3 Forgery

Forgery is "1) the crime of creating a false document, altering a document, or writing a false signature for the illegal benefit of the person making the forgery. This includes improperly filling in a blank document, like an automobile purchase contract, over a buyer's signature, with the terms different from those agreed. It does not include such innocent representation as a staff member autographing photos of politicians or movie stars. While similar to forgery, counterfeiting refers to the creation of phoney money, stock certificates or bonds which are negotiable for cash. 2) a document or signature falsely created or altered."[55]

With respect to forgery documents and signatures traditionally play an important role. In the digital world this raises the question whether electronic documents and digital signatures are entailed by the definitions in the provisions. The European electronic signature directive and the subsequent implementation in national legislation has harmonised traditional and electronic signatures, which should in principle pave the way and make forgery provisions applicable to forged electronic signatures as well[56]. This may, however, not solve everything as it may not be entirely clear whether pincodes, usernames and passwords qualify as signatures. The harmonisation of documents and electronic documents is another topic that may present problems in forgery cases. Dutch public administrative law, for instance, until recently did not incorporate electronic documents in the definition of document ('geschrift' in Dutch).[57]

---

kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het ter beschikking stellen van **gegevens met geldswaarde in het handelsverkeer**, tot het aangaan van een schuld of tot het teniet doen van een inschuld, wordt, als schuldig aan oplichting, gestraft met gevangenisstraf van ten hoogste drie jaren of geldboete van de vijfde categorie.

55 See http://dictionary.law.com.

56 Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures was published in the Official Journal of the European Communities (OJ L 13,19.01.2000).

57 On 1 July 2004, the Act on Electronic Government Communications ('Wet elektronisch bestuurlijk verkeer'), which amends the General Administrative Law Act ('Algemene Wet Bestuursrecht'), was enacted. The law regulates electronic communications between government bodies on the one hand and between government and citizens/businesses on the other hand.

In some jurisdictions a distinction is made between the various forms of forgery. The Belgian penal code, for instance, distinguishes between forgery in documents, in information technology and in telegrams.[58]

5 Data Abuse

This category contains the kind of misuse of personal data as protected by the data protection directives[59], to the extent that harvesting and abusing the victim's personal data constitutes illegal processing.

6 Imposture

"*Identity (or qualification) usurpation* means the use of a name or a qualification that is not yours. This act may be treated as a crime in its own right when the false identity or qualification is used or declared in certain types of act or deed[60], or in a request addressed to the public authority, or when the false identity is declared to a public officer[61]. This act can be also defined as "false declaration concerning identity (or concerning qualifications)" to public authorities.

Impersonation – treated as a specific crime in some legal systems - consists in misleading somebody, by assuming somebody else's identity or using a false name, status, qualification, in order to gain an unlawful advantage or to provoke damage to another (Mitchison et al., 2004).[62]"

8 Personality rights

This includes intellectual property regulations, to the extent that the name or trademark of an unrelated organisation is abused for criminal purposes. On a European scale these

---

58 Article 192bis and following of the Belgian Criminal Code.

59 European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281 of November 23rd 1995; and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Official Journal L 201 of 31 July 2002).

60 Concerning identity usurpation, see, for example, art. 433-19 French Criminal Code at http://www.legifrance.gouv.fr/html/codes_traduits/code_penal_textan.htm

61 See also art. 495 and 496 of the Italian Criminal Code:
http://www.leggiweb.it/?pagina=cerca&modalita=articolo&articolo=495&id_codice=2
http://www.leggiweb.it/?pagina=cerca&modalita=articolo&articolo=496&id_codice=2

62 See for instance art. 494 Italian Criminal Code
http://www.leggiweb.it/?pagina=cerca&modalita=articolo&articolo=494&id_codice=2

problems are governed by a number of regulations including the Berne Convention[63] and the directive on Copyright in the information society,[64] also including portrait rights.

The brief analysis of specific provisions relating to Identity Crimes shows that there is a patchwork of legal provisions that can be mapped on the stages in the ID sequence described in figure 1 (see table 2). The different European jurisdictions differ in the way they regulate the various kinds of crimes and misdemeanors related to identity and identity data.

	fishing	misappropriation	misuse	criminal action	effects
ID specific	√	√	√	√	
fraud			√	√	
forgery		√			
damage			√	√	√
data abuse		√	√	√	
imposture			√	√	
tort					√
personality rights		√	√		

Table 2. Mapping ID crime provisions on the ID frauds sequence

3.2 Some cases and legal responses

After this brief overview regulations pertaining to forms of ID-related crimes, we can now look at a couple of typical European eCommerce ID crime cases, and take a closer look at how the cases were actually handled by the legal systems. This could potentially allow the identification of certain trends in ID crime regulations, which will form the basis for our conclusion below. Our two cases involve one hacking in an eBanking context, and a series of fraudulent e-mails in which the author assumed the identities of several heads of a gambling corporation.

---

63 See http://www.wipo.int/treaties/en/ip/berne/

64 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Official Journal L 167 of June 22nd 2001).

3.2.1 eBanking and white hat hacking: ID crime with a twist

The first case[65] took place in Belgium in 2002. A Dutch eBanking user who had been living in Belgium for quite some time noticed that his bank's eBanking site suffered from some serious security issues. Due to his professional background as a system administrator, he was able to use this flaw to alter another user's account preferences. He altered the identification data of the user's frequently used accounts, so that every further money transfer by that user to these accounts would by default be directed to one of the hacker's colleague's account. During this hacking, he left a so-called "calling card", stating that the account had been hacked, and that the bank was aware of the problem.

Two weeks later, noticing that the flaw had not been fixed, he reported the problem to his local banking agency. Unfortunately, the local branch had no technical know-how, and referred the well-intending hacker to the national IT department. After contacting them, the flaw was fixed, and the hacker received a friendly note, thanking him for his help. Several weeks after that, he received a slightly less welcome note: criminal charges had been pressed, and the bank was suing him for damages.

The Dutch hacker was only sued for violation of article 550bis of the Belgian criminal code, which sanctions hacking. Unfortunately for him, this specific article does not require malicious intentions[66], and the hacker was convicted. However, keeping the good intentions into account, the judge decided to grant suspension of the verdict[67]. This type of hacking, where the hacker enters a system with the intention of finding security flaws and alerting the system administrator to them, is often referred to as a "white hat hacking"[68].

From an ID fraud perspective, it is interesting to note that the alteration of identification data was only indirectly mentioned in the lawsuit, as an aggravating element of the hacking. In this case, ID fraud was classified simply as "the use of a hacked system (altering the identification data)". No specific attention was given to privacy regulations, or the possibility of classifying the facts as ICT forgery[69] or ICT fraud[70]. Part of the reason was undoubtedly that, according

---

65 Available on-line at http://www.internet-observatory.be/internet_observatory/pdf/legislation/jur/jur_be_2004-01-21.pdf

66 Although a malicious intention (bedrieglijk opzet / intention frauduleuse) is an aggravating circumstance, the basic crime requires only an intentional act.

67 The judge also decided that the hacker did not need to pay any damages to the bank, which had sued him for compensation of the costs incurred for making the system safe. The bank's logic was that, if the hacker had not committed his crime, the system's weakness would not have been revealed, and therefore these expenses would not have been necessary. The judge rightly rejected this line of reasoning. Although this is certainly interesting, it is not directly related to ID crime and will therefore not be further examined in this paper.

68 Etymologically, the expression is said to be based on old Western films, where the heroes typically wore white hats. Their nemeses, in contrast, would frequently wear black hats, and this, too, is a label adopted by the malicious elements in the hacking community: black hat hacking.

69 Article 210bis of the Belgian penal code.

to Belgian penal law, only the strictest punishment is applied in case of multiple infractions, which would have rendered the additional (no more strict) qualifications pointless. Additionally, the novelty of the hacking crime in Belgian law was likely a factor. Anti-hacking legislation clearly applied, and considering the relatively limited seriousness of the offence, additional qualifications were likely considered inappropriate.

Regardless of the actual reasons, the only real conclusion can be that, in this specific instance, ID crime was adequately fought using generic ICT crime legislation.

3.2.2 e-mail ID fraud and gambling

In a more straightforward example of eCommerce related ID theft, the French gambling organization Groupement d'Intérêt Economique du Pari Mutuel Urbain (GIE PMU) was confronted in September 2001 with a series of e-mails claiming to contain enough information to hack into GIE PMU's systems and transfer large sums of money[71]. Part of the information appeared to have been captured during an earlier hacking in November 2000. The mails contained extensive documentation describing the technical details of the company's computer systems, as well as a large series of usernames and passwords of (ex-)employees of GIE PMU. A brief check of this documentation showed that the information was largely accurate, if somewhat dated.

The mails were sent out to GIE PMU's employees, and its contents were published on a website in December 2001. Despite the attention given to this turn of events in the national press, no hacking attempts followed. A second series of e-mails was sent out in March 2002, again containing the sensitive information. The perpetrator(s) who were responsible for the hacking and/or the e-mails and website were never identified[72].

The sender of both batches of e-mails had spoofed the from-addresses of the e-mails, to resemble the addresses of certain employees of GIE PMU. This is a common ID theft technique in fraudulent e-mails (also used in the phishing example above), through which the ID criminal hopes to inspire a certain trust in the receiver based on the false assumption that the mail originated from a trusted source. Whether or not the forging of the from-addresses had any measurable impact in achieving the sender's goals (including damaging the reputation of GIE PMU) is debatable.

An interesting question is whether the assumption of another person's identity to inspire a false sense of trust can be considered an ICT offence. As we will discuss below, this is not

---

70 Article 504quater of the Belgian penal code.

71 The mails made various claims, the most extreme example promising a possible return of 35 billion FFR (roughly 5 billion €).

72 Two major elements in impeding the investigation were the relative age of the data connected to the first e-mail (more than one year old, so that no verifiable logs were left), and the fact that the second e-mail was anonymously sent from a cybercafé.

completely certain. E-mail ID-spoofing seems to be an example of a violation of the privacy directives, and since the data was acquired through hacking, the Cybercrime convention's rules regarding illegal access also seem to apply, yet we will a more detailed account of this matter to section four.

Obviously, this specific case could not yield a clear ruling on the exact applicability of French law, as there was no identified suspect, and the court had to limit its role to suspending of the proceedings until such a time as the perpetrator(s) could be identified. However, the judge's ruling does specify the exact allegations: the unidentified intruder was accused mainly of illegitimately accessing and maintaining himself in another person's computer system (i.e. hacking)[73], obstructing the proper functioning of the system[74] and violation of trade secrets[75].

Again, it is remarkable that the prosecution of a case that clearly encompasses ID crime aspects tends to focus on other elements, in this case most notably hacking. In part, this is likely related to the fact that hacking is the most well known form of ICT crime, whereas ID crimes occupy a fringe position. Quite possibly this will change over time, as the prevalence of ID crime increases and European prosecutors and judges alike become more aware of its significance.

3.2.3 Legal frictions?

The examples show that that prosecution of the imposters did not take place on the ground of ID fraud of theft, but instead on either entering a system that contains ID data (hacking) and on crimes related to the consequences of this entering (obstruction, violating trade secrets). In the light of the sequence of ID-related crime as presented in figure 1, this primarily concerns phases one and four (criminal action). Whether this is due to the fact that specific provisions with respect to ID fraud do not exist, or due to procedural matters (for instance, the chance of success in getting a conviction), or priorities of the courts involved, remains to be seen.

In any case, the cases above give the impression that the ID-threatening aspects were considered to be symptomatic of other crimes, sometimes as aggravating factors, but rarely worthy of prosecution in its own right. Perhaps this is due to the specific subject matter: as this section of the paper only examines eCommerce related cases, it stands to reason that the parties involved would be more likely to resort to the most obvious solution. Typically, this implies a classification that is immediately and obviously applicable, such as hacking, rather than a more complicated classification as a violation of privacy.

---

[73] Article 323-1 and 323-5 of the French penal code: *accès frauduleux* and *maintien frauduleux dans un systéme de traitement automatisé de données.*

[74] Article 323-2 and 323-5 of the French penal code: *entrave au fonctionnement d'un système de traitement* automatisé *de données.*

[75] Article 226-13 and 226-31 of the French penal code: *violation du secret professionnel.*

3.3 Conclusion

As we have seen in the examples, the problem in tackling identity crime rarely lies in the lack of suitable legal provisions. Rather, the situation is exactly the opposite: most incidents of identity crime will be covered by a multitude of provisions, allowing the prosecution to take its pick. The failure to adequately stem the increase of such crimes originates from a different problem: the inability to consistently apply these provisions in practice and the lack of a comprehensive integral framework.

In fact, this is a problem that seems to rear its head in any form of cybercrime: criminals have the distinct advantage of always being at the forefront of new technological developments, allowing them to exploit a seemingly endless stream of technical loopholes to manipulate their victims. And even when no such loophole is available, a combination of social engineering and the lack of security awareness in the average user offers a plethora of criminal opportunities. Add to this the simple fact that national borders are all but meaningless in the information society, and an almost ideal situation has presented itself.

Law enforcement agencies on the other hand have to deal with limited budgets, difficulties in keeping up with identity criminals from a technological perspective, and inefficiencies resulting from the need for cross-border collaboration. Thankfully, positive steps have been undertaken to remedy some of these difficulties (e.g. by the establishment of national computer security incident response teams, and more recently the establishment of ENISA[76]), but a great deal of work still remains to be done. This is especially true for cross-border law enforcement collaboration outside of the European Union.

Additionally, there is an insufficient consensus on the importance of privacy protection. While the European data protection directives have greatly strengthened the European legal framework, the strict application of this framework is not always considered a priority. Outside of the European Union, no international consensus exists on the importance of the protection of personal data as such, although awareness of this issue seems to be increasing.

While the legal framework still offers room for improvement (especially where international collaboration is concerned), it seems clear to us that the current trend of rising identity crime can not be stopped through legal action. Rather, a hybrid solution combining legal response mechanisms with technical measures seems in order. The development of new identification techniques, such as the use of biometric identifiers, certainly offers some possibilities in this regard, as does the increasing acceptance of technical aides such as digital signatures.

And finally, the role of user awareness should not be neglected. After all, no additional security mechanisms will ever aid a user who is not convinced that his personal data is worth keeping safe.

---

[76] The European Network and Information Security Agency; see http://www.enisa.eu.int

4 Social and Economic Aspects

4.1 Introduction

Nowadays, people have offline and online lives, and in each they use identity information to access services. Identity allows individuals to perform different essential roles in society (e.g. voter, employee, customer, e-customer, e-client of bank, etc.). Therefore, in view of defining identity, we have to distinguish between offline and online identities and how they are related. Offline identity information can relate to appearance such as hair colour, eye colour, glasses, etc.; it can be social information, e.g. name, postal address, phone number; or it can be represented by identity tokens, i.e. passport, visa, credit card, social security number, bank account number. Online or digital identity can be described in the same way. The information related to the appearance can be incorporated into, for instance, a digital biometric template (fingerprint template, iris template). The corresponding social information can be a nickname, an e-mail address or an IP address. And digital signatures or certificates can be considered as identity tokens for digital identity.

Identity information to bridge offline and digital identities is essential because it plays the role of the interface between offline and online life. Identity information can further be distinguished in information that provides 'knowledge-based' identification (e.g. password, PIN) and information gathered from the user context (e.g. profile, user preferences) that links implicitly without consent of the person identified by the data.

Possessing an identity allows individuals to act in society, and hence adopting someone else's identity is beneficial to some people. ID theft has always existed, throughout history examples of identity takeovers are recorded for instance.[77] But the advent of the Information Society has dramatically multiplied its occurrence. Technology facilitates the reuse/misuse/usurpation of identity information as it replaces face to face contact and the social checks and conscious processing of personal data that accompanied traditional face to face interaction.

Identity theft is a breeder offence that may lead to identity fraud. Unfortunately, individuals are often unaware of the range of impacts of identity fraud. Identity theft and identity fraud not only concern and affect individuals, but also companies. The main threats here are company takeover and cloning. Furthermore, considering the increasing use of networks (Internet or other networks to exchange information) and the lack of control, the utility of identity theft has grown and anonymous identity fraud is facilitated and may proliferate. Identity theft and identity fraud are therefore important security issues.

In this section, we first define and explain identity theft and identity fraud in detail from a sociological point of view. We also study their social and economic aspects and impacts,

[77] See http://www.caslon.com.au/idtheftprofile1.htm#literature for an interesting overview.

whether tangible or intangible, related to the private or public sector, and finally, we provide an overview on initiatives for countermeasures.

4.2 Identity Change, Identity Fraud and Identity Theft from a sociological point of view

The definition of "identity fraud" is often primarily attributed to the existence of damaging motives or actions of an "identity fraudster". The disadvantage of this definition is that, on the basis of the persons' actions, the motive can be concluded or assumed only indirectly. In this chapter we extend the scope of analysis and introduce a categorisation of types of "identity fraud" on the basis of an operative approach that connects the various types of "identity fraud" with socially observable facts (within processes) of addressability, expectation concepts and authentication procedures. This enables a perspective for

- inspecting the types of adequate addressing (e.g. if it is directed personally or by use of the broadcasting method),
- understanding the reasonableness of certain expectation concepts for typical, socially different situations with regard to their functionality, scope, and purpose, and
- observing and evaluating the different authentication procedures and their risks in different types of social systems.

This approach not only allows us to define the various types of identity fraud, it also enables us to provide a more detailed description of possible counter measures than the approach that relies on people's motives. The construction of different methods of address creation, creation of expectation, and authentication procedures of the different types of social systems can be used as the starting point for the development of counter measures.

4.3 Establishing persons as entities in social systems

Persons

From a traditional socio-psychological point of view we have to think of a person as an individual which has a body, has a view of himself in difference to others (Freud, 1978) and a "Core I", which is typically constructed as the source of a free will (Mead, 1934) From the social psychological-perspective and basing on the "Core I" understanding used here, identity is the difference between the physical body of a person at a certain time (past, present, future) and the self-consciousness of this person (I am myself, and I am the same person that I was in the past and that I will be in future). In other words, the identity of an individual is constructed as the operative difference of sameness as an object in time and selfness in its consciousness. Strictly speaking, only particular partial identities are affected by theft and

fraud, the "Core I" is left unaffected. We will therefore focus our analysis on the "Me-related" parts of identity that are relevant for social interaction.

Social systems

From a radical sociological point of view, the identity of a "person" (Luhmann, 1991) is a construction in a specific situation that largely depends on the social system in which this construction occurs. Social systems are pools of schemes, events and communicational components. These elements shape the behavioural and communicational repertoire of actors within the given social system. By adopting roles compatible with the adopted social system, such as customer in an economic (shopping) system, and by using the communication patterns associated with these roles, the identity of a person is defined. The relevant characteristics, or partial identity, that make up a person's identity therefore depends on the social context.

Sociologists distinguish at least three types of social systems:

- *Interactional systems* (types of communities in which members are not subject to particular rules, but nevertheless schemes apply; examples are spontaneous meetings as neighbours, spontaneous encounters) (Kieserling, 2000),
- *Organisational systems* (characteristics are membership and effective production of decisions; examples are public bodies, institutes and companies) (Luhmann, 2000; Baecker, 1999),
- *Functional systems* (economy, law, politics and science as "self-conducted" communication systems) (Luhmann, 1997).

Social *functional systems* reproduce particular patterns of communication that have particular social functions (e.g. buying and selling, political debate). These functions, in turn, define meaning (original German term: *Sinnhorizonte*) for organisations, which create particular sets of expectations (role conformity as "customer", "citizen", "responsible citizen", "human being") for the persons acting in them.

Functional system	Fundamental decisions	Programme	Generic role (person) e.g.:
Economics	payment / non-payment	Products & prices	Customer, vendor
Legal system	legal / non-legal	Legislation	Citizen, judge
Politics	power / non-power	Political programmes	Responsible citizen in the meaning of the French term 'citoyen'
Science	true / false	Theories & methods	Human being, expert, laymen

Table 3. Social functional systems

Organisations generally operate in different social systems at the same time, but they have a main emphasis in one. A shop, for instance, primarily operates as an economic system, but may be involved in a political system when proposed changes in zoning plans endanger its existence. The primarily economic target of the shop remains unaffected by this political engagement.

From the perspective of social systems, communication thus involves actors in socially typical processes, e.g. as citizens of a certain country, as a company's customer, as a patient in hospital or as teacher in a school, but also as "my friend", "my mother" or "my neighbour". The role adopted by the actors is defined by the current social system, but often multiple social systems are at stake, e.g. during my criminal trial I happen to notice that I know the judge, we went to high school together, and hence the proper social system has to be selected. Selecting the proper context is partly done by addressing, for instance, I could in principle address the judge as 'your honour', but also 'Jim', my old high school friend, which would result in selecting either the (proper) context of a legal functional system, or the improper interactional system of a friendship. Apart from the addressing mode, also authentication and authorisation play a role as this functions as a gatekeeper to a particular social system. I, for instance, am not a judge. Imposing to be one would place me in a social setting where I should not be able to act. In this connection, addressing, authentication and authorisation is not to be understood in a pure technical sense as partly defined in chapter 6, but also extendedly referred to the social context. We understand the technical concepts of addressing, authentication and authorisation as incarnation of social structures.

Addressing, authentication, and authorisation

In the following we examine typical processes of communication in different social systems to gain an operative understanding of the processes and mechanisms of "identity fraud" and "identity theft". The examples have been taken from the physical world. We describe persons in interaction systems as *participants*; persons in organisations as *members*; and persons who interact as externals with an organisation as *clients*.

Interactions in the offline world typically arise when the participants are within hearing range and communication takes place by use of speech. When the participants in such an interaction know each other's names they will use these, or in particular situations nick names or pet names, to **address** each other, usually preceded by a salutation ("Hello Mike!" or "Hi Babe"!). The name functions as an identifier[78] of the addressee. Instead of names, people also use bit strings that are frequently introduced to be able to address a person in a unique way (cp. chapter "Identity collision and identity change").

Merely addressing a person by an identifier does not guarantee that this person actually is the one to which the identifier 'belongs'. Hence, some form of **authentication** takes place to establish the proper linking of identifier to known person, for instance through inspection (looking in each other's eyes), but also, listening to the tone of voice, interpreting gestures, etc, play a role in verifying particular identity claims, the intention and its authority. When a particularly high claim for commitment is connected with a communicational relationship, for instance on a friend, the authentication and authorisation processes for the identification of who the specific person behind the role is and which rights they are entitled to within an interaction typically becomes lengthier. Authentication/ authorisation within social systems maps very well concerning its function and the use of different levels to authentication/authorisation used in technical systems. In this case intimate communication among the friends at the beginning of a communication, for example the exchange of a shared communicational history, can be part of this authentication/authorisation procedures aiming at planned future interactions.

Especially when the actors involved show different (or at least insufficiently specified) expectations, when role collisions are so to speak structurally very likely and an equivalence of motive and type of action is very unlikely, authentication and authorising procedures are deployed in a more deliberate and stronger way. It depends on the result of the authentication whether the supposed role collision can be solved or if it results in a role conflict.

Generally speaking, we distinguish between the following three levels of authentication and authorisation:

---

[78] Abbreviated as ID; names or other bit strings, in this case partial identity linked to a person or possibly to a role. In other contexts IDs can also be linked to hard- and software.

- the social level (related to the social system and the role taken there)
- the personal level (identification of the person)
- the technological level (through technological authentication and authorisation procedures)

In the online world, the social and personal level of authentication have lost their nonverbal aspects (tone of voice, gestures) of communication, and authentication generally has to rely on written claims. This makes claims more difficult to prove, especially since what results are merely bit streams that can in principle be generated by anyone. As a result of this loss of quality of the social and personal levels of authentication, the technological mean s of authentication gains importance.

Authentication and authorisation in general rely on four factors:

- integration into the social system
- assignment of the role
- identification of the specific person, the personal authentication
- generic (related to the role) or personal assignment of opportunities for action (rights), the authorisation

The required level of authentication/authorisation depends on factors, such as, the nature and content of the communication (e.g.: open discussion or private exchange? Is the content confidential or not? Private sphere of one or more participants in the communication affected?), the kind of social system (Is the main system interactional or organisational? Which functional system is involved?), etc.. In interactional systems, for instance, usually a simple person-related mode of addressing by the participants is sufficient for most interactions (conversation). This type of addressing is also generally used by organisations towards their clients.

Within organisational systems, additionally, function-related addressing is used. This allows the production of structures and ways of communication within organisations and to their clients (external communication to persons or other organisations) that establish clear expectations. A specific person is involved if an individual is addressable in interaction with other individuals or organisations. Apart from addresses, there are general organisation-related role concepts, such as "citizen", "client", "the human being" or "responsible citizen".

As far as persons are concerned, organisations are characterised by the fact that persons act as their members. Persons are function bearers who are internally addressable by use of particular way of addressing (departments, head, staffer or special designation) and who are addressable from outside in a similar differentiated way and via the organisation's generic

address. Organisation-specific communication is orientated towards decisions or the creation of the ability to decide. Decision-orientated communication is the general feature of all organisations. In general, it takes place in written form and is actionable, economically calculable, can be recorded scientifically (e.g., statistics, models and simulations) and forms the medial basis for further decisions. The authentication procedure is often quite simple and based on the analysis of the course of communication. This course is to a great extent structured by the fact that the person involved is a member or a non-member of the organisation. In this connection, the member/non-member (or insider/outsider) concept works in a resolution which is becoming higher and higher in progress of the communication. Knowledge about persons, which is revealed by calling them by their names and can absorb addressing, authorising and authentication aspects from interactional systems as a side effect, is consulted for decisions, as an authentication reference, so to speak. Forwarding by superiors or co-workers or the seemingly legitimate access to resources owned by the organisation (letterhead, e-mail sender, file access, but also keys and ID cards) play a similar role.

Interactional systems generally use other types of authentication and addressing than organisations. Therefore, different types of "identity fraud" may occur in both types of systems.

4.3.1 General properties with respect to rearrangement of identity linkage

In this chapter we not only elaborate on identity theft and "identity fraud", but on the broader area of rearrangement of identity linkage, i.e. every modification concerning the link between the identifier of a (partial) identity and the person[79] who is identified by this identifier or who is the bearer (or holder) of this identifier. In a typical setting the identifier of a person (or the person's partial identity) is being linked to another person. As the widely used terms identity theft and "identity fraud" do not distinguish between identifiers and (partial) identities, the terms proposed in this text are built in a similar way. From the context it will be clear that in most cases the focus is on the linkage of identifiers which point to a partial identity, e.g. consisting of personal data and attributes, possibly including reputation information or authorisations.

Although the full analysis of all possibilities extends beyond the scope of this text, we give a flavour of structural elements which could be further elaborated in further studies:

- In general there are different subjects concerned which have to be identified in each constellation:

[79] Possibly extended to roles instead of persons.

  - An original identity bearer, i.e. the person who used the identity originally[80]
  - A non-original identity bearer, i.e. the person who uses the identity originally assigned to another bearer or a non existing identity (e.g., a non-original identity bearer or identity creator)
  - Possibly: third parties involved, e.g., with a relationship to the original identity bearer or the non-original identity bearer, or observers of related incidents.

  For each subject it is relevant

  - who initiates the rearrangement of identity linkage,
  - who knows about the rearrangement or can find out, or
  - who may profit or may suffer from the rearrangement.
- Besides the subjects concerned there are important objects, especially:
  - Identifiers, which play the main role in rearranging the identity linkage,
  - Personal data,
  - Personal and role attributes, especially reputation or authorisations, and
  - Actions, e.g. communications or transactions with other parties.
- In exceptional cases there might be no persons who bear or receive identities. This is e.g. the case when a person in the internet creates up a valid credit card number which is not linked to an account.[81] This person may then act with the authorisation as if there were an existing account until the other party checks at the bank. Here we see that the part of the identity which is used by a non-original identity bearer may not only comprise personal data, but even authorisations without any personal linkage.
- What is the focus: the process of "rearranging the identity linkage" (e.g. taking/giving the identity) or "use of the identity"?
- Is it done intentionally (by whom?) or does it happen accidentally?
- Does it happen with consent or (explicitly) against the will of the subjects concerned?
- Is the rearrangement of identity linkage unilateral, i.e., one identity is rearranged, or are more identities concerned, e.g., to swap the identity so that the original identity bearer is a non-original identity bearer, too, and vice versa?
- Is there a unique (1:1-)linkage to the identity or may the linkage be non-unique (before and/or after the rearrangement)?
- Is the rearrangement of identity linkage legally relevant or not?

---

[80] We tried to use neutral terms. In typical constellations terms might be used which reveal the perspective of the observer, e.g., identity theft or victim.

[81] Most credit card numbers contain a check digit. A simple algorithm is applied to the other digits of the number which yields the check digit. See, for instance, http://www.faqts.com/knowledge_base/view.phtml/aid/3103.

- Do the subjects (possibly) have wrong assumptions on the identity linkage whether it was rearranged or not? What may be the consequences of these wrong assumptions?

In the following we concentrate on main constellations. Our first distinction is the intention: Does the rearrangement of identity linkage happen accidentally (identity collision) or is it done intentionally (identity change)?

4.4 Towards a typology of rearrangements of identity linkage

In this section we describe various types of rearrangements of identity linkage with the target to get a better understanding of identity fraud and identity theft. In this context we examine identity collisions, changes[82], deletions and restorations. Identity collisions, deletions and restorations are not described in depth and comprehensively; they are introduced to get a better understanding of borderlines between various types of rearrangements of identity linkage.

4.4.1 Identity collision – definition and types

Legally not relevant, but frequently observed, is a series of identity-referred errors occur which we categorise as **identity collision**. All types in this category have in common that they take place without intention on the part of those involved.

We can distinguish between the following three types of identity collision:

- identifier collision
- linking error
- role error including role collision

An **identifier collision** can happen when the same identifier is mapped to different persons or roles, i.e. the identifiers are not unique per person/role. A typical example of this type is the equality of names of two different persons, which leads to a mixing-up by third parties.

A **linking error** can happen if an identifier is assigned to the wrong person, e.g. if an identifier is wrongly assigned to a person by mistake because of the similarity of two identifiers that are related to two different persons. Examples are the use of wrong e-mail addresses or mixing up address data, the incorrect recognition of persons in the street or the mixing-up of parents with their child on the telephone due to the similarity of their voices.

---

[82] In this case we understand identity change as change of the linkage of an identifier to a person or a role within a social system. Identity change also is discussed as change of a partial identity of a person over a period of time in sense of evolvement etc..

A **role error** can happen by an incorrect assignment of the role. One example for this is a citizen going with a specific request erroneous to a public authority and to a specific office clerk, that is not concerned it this matter.

Role collisions are special cases of role errors. They can happen when different expectations are placed on the persons in the social interaction and these expectations are not met by some or all of those involved (as long as they are not expressed explicitly), which then introduces a conflict.

A typical example of a role collision concerns situations in which one of the actors implies the existence of a friendship that can handle stress, because signs within the communication make him believe this, whereas the other actor interprets the signs differently. This may result in different expectations of both actors with respect to the respective rights and obligations of the parties.

Another typical constellation of a role collision is one in which possible role changes are not performed simultaneously by the actors involved. This happens, for instance, when a long-term friend does not sell a car to his friend as a friend, but in his/her other role as a professional car dealer and aims at a from his professional perspective optimised price. If the buyer is unaware of this role change, his hopes for favourable conditions may be undeserved. Unless the communication makes explicit the different expectations, such a role collision – which often remains undetected – may result in a conflict or recurring conflicts.

4.4.2 Identity change – definition and types

Identity collision, which occurs unintentionally, can be distinguished from intentional changes of identity, which we will call the **identity change**. We understand identity change and the related subcategories from the perspective of the person that actively performs the identity change. This could be the original identity bearer, the non-original identity bearer, a third party, or combinations thereof. The perspective of the subject whose identity is affected (the original identity bearer; if there is malicious intent: the victim) is much more complicated. We describe subjects behaving passively to the identity change as targets. Various types of identity change can lead to one or more targets for the performed identity change.

We can distinguish between four, closely related[83], types of identity change:

1. identity takeover

[83] As we will see in section 4.5.

2. identity delegation[84]
3. identity exchange
4. identity creation

Identity takeover characterises taking an existing identity of another person without this person's consent. Typically the identity taker[85] (i.e. the non-original identity bearer) uses the identity of one party (one side) in an already established relationship in which those involved have justified expectations with respect to the workflow and its results. A typical example of this kind of identity usurpation is the adoption of an existing client's identity in relation to an organisation. The identity taker can take an identifier, such as the social security number, a credit card number or the login of the existing person to impersonate this client. In cases such as these, either the authentication phase of the victim has already passed, or it can be handled easily because of the identity token. In each case, the operatively accessible characteristic features of the usurpated identity are accepted by all the parties in the interaction. By this acceptance, a certain course is determined to which both sides adjust their expectations deliberately. An identity taker thus practically takes over one side of an already existing communication relationship, or joins in on the communication without the victim's (initial) awareness.

There are always two targets in cases of identity takeover. *Target 1* is the person whose identity is taken, the original identity bearer. *Target 2* is the person who was tricked into believing that the identity taker is the person he impersonates.

Identity takeover does not always have to be illegal in a strict sense, e.g. in public sketch situations (practical jokes with a hidden camera etc.). The sketch is often based on an actor assuming (simulating) the role of a function bearer or an official (Target 1, identity capture) and starting a communication with citizens (Target 2) in a role-specific but excessive way.

Based on the proposed definition of identity takeover, dissociation is possible, too. According to this definition, third-party logging of user data, e.g. for the purpose of generating profiles, is clearly no identity takeover. Partly, there may be unique identifiers (e.g. globally unique identifiers; GUID) collected and stored in connection with user data of Target 1. However, these data are not used to impersonate Target 1 in an already established communication relationship between Target 1 and others (possible target 2's). The use of these data takes place either internally related to one's own communication relationship with Target 1 and in cases of transmission of profile data to third parties in other communication relationships of

---

[84] As an alternative term „identity licensing" was suggested in the Tilburg workshop.

[85] In a general sense, this is not necessarily a person ('client'). Institutional actors, such as spies acting in their professional capacity, can act as identity takers (in this case interior culprits).

Target 1, or in new communication relationships in which the phase of authentication has not been completed yet.

In the following, we use the term **identity delegation** for situations where the person whose identity is taken over (Target 1; the original identity bearer) has consented in the takeover. Therefore, this type is the mirror case of identity takeover as identity takeover lacks target 1's consent. A typical example of identity delegation is lending one's credit card and PIN to one's spouse to enable them to withdraw money from Target 1's account. Usually, an identity delegation is bound to a limited period and a purpose. It can be observed in interactional systems but is also used in organisational systems, e.g. with deputising actions (such as e-mail forwarding).

A special case of identity delegation is represented by identities (more precisely: partial identities that can be used as identifiers) that are made available to a group of persons. Since linking these identities with specific persons within this group is no longer possible. This scheme allows for anonymity. A number of internet anonymity services (AN.ON, Tor etc.) use this principle.

Another case that resembles identity takeover is **identity exchange**. This typically happens in existing, stellate (e.g. 1:n-)communications, for instance in communication between an organisation and their customers. Within such a relationship, two bearers of the same role (e.g. customers) exchange their identity actively towards the other communication partner (e.g. the organisation).

Identity exchange is used by, for instance, CookieCooker, which exchanges cookies related to a website randomly between different CookieCooker users. In this way, the site owners' possibility to generate usable profiles on the basis of the cookies is evaded. Identity exchange in this example is characterised by the fact that it happens with approval and only for a particular purpose (namely the covering-up of profiles).

The above-described types of the use of already existing identities can principally be distinguished from the creation or construction of a new identity that proves (concerning the method already used in the past) to be able to pass an authentication procedure. In the following, we use the term **identity creation** for this. In this perspective, the culprit has to understand and master the authentication phase as a valid identity (token) has to be created. An example of identity creation is the construction of a credit card number that passes the validity test (see note 81), although not too many people will be fooled by this, as additional checks on name, expiration date and the validation number will usually be carried out.

Identity creation does not need to be the result of criminal motives, the use of pseudonyms and "virtual identities" in the sphere of avatars are perfectly legal examples of identity creation. These partial identities in artificial (and also virtual) environments are deliberately not (to be) linked with their holder's real identity and their "Core I".

Identity creation and identity takeover may collapse from an observer's point of view. A newly created ID from the perspective of its creator may well already exist in the sphere of the observer. This frequently happens when one is to create a user name for a service. Even identities that may appear highly improbable sometimes turn out to exist already, hence these services are frequented by people whose ID is something like Jones123. When noticed by the identity creator the identity collision can be repaired. If not, the result may turn out to be identity takeover.

4.4.3 Identity deletion

From the social perspective deleting a (partial) identity means that the communication of the person via this identifier terminates and that the person thus no longer is not connected to the related social systems. Identity deletion can be performed accidentally or can be intentionally. In addition, identity deletion can (like authentication) be actively performed by the original identity bearer, or caused passively by someone else. As performed by someone else, passive identity deletion can have severe consequences for the person whose identity is deleted. Identity deletion without the subject's consent is not necessarily undesirable. If a member leaves the organization (for example when an employee changes employer), partial identities, such as the link form the person to an internal functional addresses, or the deletion of an internal telephone number, are usually passively deleted. This erasure of records within the organization often does not involve the subject's consent.

As identity deletion is a case of unlinking an identity, instead of relinking (or linking in the case of identity creation) an existing identity, with different kinds of consequences, we treat identity deletion as a separate category instead of a subtype of identity change.

Following this definition, many cases that are discussed to be identity deletion, such as e.g. the abolishment of ID documents by illegal immigrants, are no identity deletion. These cases can be best be understood as the first step towards identity creation; illegal immigrants want to live in a new country with a new personal identity, and hence enter the social system of the new country, instead of leaving it, as would be the case in with identity deletion. From the perspective of the refugee's former country of residence, it is a case of identity deletion, but that is not the perspective in which this kind of abolishment of ID documents is usually addressed.

In accordance with this definition the revocation of a digital signature certificate by the owner is **active identity deletion**. The declaration of the death of a person in a newspaper or towards public authorities is **passive identity deletion**. As long as the person is really dead this is a legal procedure e.g. performed by close relatives. In cases of malicious intent, passive identity deletion in this example is a personal offence.

4.4.4 Identity restoration

Related to identity deletion is identity restoration. We understand identity restoration as the reintroduction of a partial identifier that was previously deleted for some reason, for instance by accident. Identity restoration usually is intended. Successful restoration results in an identifier that can be reused again to its full extent in the appropriate social context. Identity restoration, like identity deletion, can be performed actively by the person who originally was linked to that identity or passively by a third party.

Identity restoration collapses with identity takeover if done without the subject's consent.

4.5 "Identity Fraud"

From this general sociological perspective, **"identity fraud"**[86] can be defined as**:** to claim the fulfilment of someone else's legitimate expectations concerning one's own identity, role and behaviour within a specific communicational context, but to only simulate the others' expectations towards them, and thus to evade these expectations deliberately. From a legal point of view, fraud requires deliberate action as described in chapter 3.

Therefore, there is no "identity fraud" to be expected in the area of identity collision but, above all, in the area of identity change (deliberate action!). In this respect, we understand "identity fraud" as a subcategory of identity change.

On the other hand, identity fraud is usually understood as a main category of **"identity theft"**[87]. In general, identity fraud is typically an illegal fake of a particular person's identity towards another person or organisation. In this general sense of fake, this applies to identity theft, too. Therefore, identity fraud is the general term for the faking of an identity by use of identity change, e.g. with reference to a client-organisation relationship, and identity theft is the more specific term for the special case of an illegal capture or usurpation of an already existing identity.

The following figure will show the described relationship between the introduced terms.

---

[86] Identity fraud means "that someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non-existing person" (J. Grijpink, *Identiteitsfraude als uitdaging voor de rechtstaat;* Privacy & Informatie, August 2003) [translation Bert-Jaap Koops]

[87] Criminal record identity theft occurs when the identity thief obtains a victim's personal information and then commits crimes, traffic violations, or other illegal activities while acting as the victim. Instead of providing law enforcement with her own personal information, the identity thief provides the victim's personal information in order for the identity thief to avoid criminal convictions and legal sanctions in her own name. (Perl 2003, p. 169)

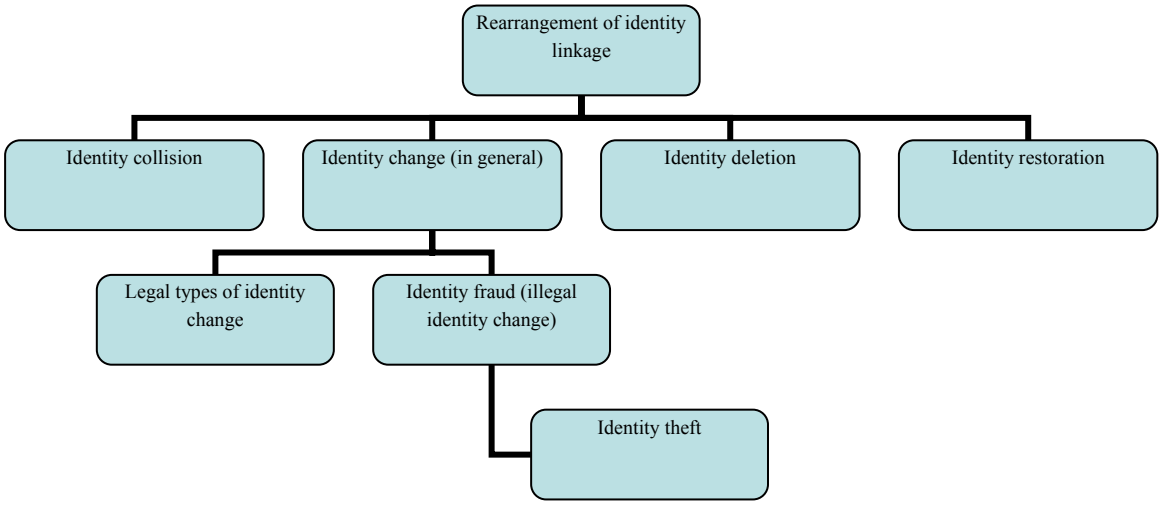


Figure 4. Introduced terms and their relationship

Systematically, the four introduced types of identity change can be examined for the existence of a deceitful subcategory. Should that be the case, we suggest modified terms.

Identity change	**"Identity fraud"**	**Comment/ common features**
Identity takeover	Identity theft	Feature: Missing agreement of original identity bearer.
Identity delegation	Deceitful identity delegation	Example: Credit card misuse, where the card holder actively issues all necessary information to someone else and claims to be victim of identity theft to avoid payment; misuse of a delegated identity beyond the agreed purpose leads to identity theft Feature: The original identity bearer has agreed.
Identity exchange	Deceitful identity exchange	Example: Identity exchange for the purpose of creating alibis Feature: Mutual agreements by those whose identities have been exchanged (i.e. by both original identity

		bearers).
Identity creation	Deceitful identity creation Rarely used: "synthentic identity fraud"[88]	Example: Creation of credit card data (number, name, certification number) Feature: No original identity bearer is expected to exist.

Table 4: Types of "identity fraud" and their assignment to the types of identity change

The comparison between the currently used definition (see note 86) of "identity fraud" and this overview (see table 4?) results in an extension of these terms. This applies to the illegal identity exchange and delegation, in which – in contrast to the cited common definition – two actors are involved. As far as the following criminal acts are concerned, the partner in the illegal identity exchange thus becomes an accomplice.

In all, this assignment allows a more detailed view on the origin of the identities that are deployed for purposes of fraud as well as the communicative environment in which they can be deployed. In the following, this is to be examined more closely from a sociological point of view.

4.5.1 "Identity fraud" in social systems

"Identity fraud" in social systems means a deception of the role assignment (e.g. by inspection), or of the subliminal examination of the existence of the common understanding of the social relationship. After all, even loving relationships require proofs of love every now and then. Therefore, an identity fraudster has to dress up as somebody else (identity theft) or, as a sort of special social trust advance, to pretend to be particularly trustworthy, typically by use of confessions, or to acquire particular trust by fulfilling expectations over a long period (deceitful identity creation). Due to the personal and social effects to be expected on the provider, deceitful identity exchange or delegation are probably of secondary importance. In these cases the original bearer of the identity will always be a starting point for incrimination in the following criminal investigation. This makes these types of identity fraud less attractive for them.

"Identity fraud" within an organisation means the assumption of organisational membership by a fraudster, which, in contrast to interactional systems, is not made possible by confidentiality and inspection but by the sovereign handling of resources, adopted to the common social manners within this system (e.g. "The Captain of Koepenick", a novel by Carl

[88] http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/02-09-2005/0002989118&EDATE=

Zuckmayer, who describes this impressively[89]). A classic regulator for closeness-distance relationships in organisations is joking or, even more promising, joking about weaknesses of workmates or the organisation, based on precise observations. In a shared joke, agreement is communicated in a non-binding way.

Trends indicate that the authentication procedures become more formal, depending on the extent to which the core operations of an organisation can be affected by access. Also in these situations, identity fraudsters will use their social competence ("social engineering") to obtain access instruments for resources (login, ID card, signature, key access). Depending on the extent to which identification and authorisation of people is required within organisations, identity theft is more likely to be observed than deceitful identity creation. For the same reasons as in interactional systems, deceitful identity exchange and delegation are probably of minor importance.

The internal relationships of members within an organisation are to be distinguished from the external relationships of organisations with each other or between organisations and their clients. The latter are typed by use of patterns such as seller/buyer, client/supplier, citizen/official or in the different incarnations of the layman patient/expert constellation. Due to the mutual expectations created by these social contexts, the processes are highly standardised. In the described relationships those involved perform in favour of each other. Therefore, the communicational processes are regulated by contracts, economically calculated and / or scientifically measured. An identity fraudster does not only evade the expectation that something in return will be offered (money, obedience, truth), as implied by the social conventions, but they also evade the sanctions, because their true identity cannot be established despite the fact that they appeared as a person which allowed them the opportunity to deceive. This makes the identity fraudster different from a thief or burglar who remains unrecognised and typically avoids appearing as a person and thus avoids authentication / authorisation in social systems completely.

Since the danger of personal sanctions to be feared is rather small, especially for a client, deceitful identity delegation and exchange can probably be observed in this constellation of extra-organisational relations, too. To a member of an organisation in interaction with clients, this probably applies to a much smaller extent; the conditions here rather correspond to those within an organisation.

Authentication and authorisation between an organisation and its clients is often lax or absent. Despite the fact that organisations can place restrictions on access, and that instructions are to be followed (registration, for instance), many actions, such as purchasing with cash money,

---

[89] In this story a former convict needed a passport to get a job, but is allowed only to get a passport, when he has a job (a paradox). He bought the uniform of a captain in a second hand shop, took some soldiers from the street under his command and seized the town hall with the target to get a passport there.

casting political votes, and accessing scientific publications, can be done anonymously, or at least pseudonymously. Even in places in which conventional authentication by use of technological means is in place, this is often unreliable. ID cards can be falsified, particularly with the meagre biometrical quality of photographs, and controls are only unreliable. Orders can easily be placed under the pretence of false sender address, by letter and on account, also in the name of another person. Account, tax and social security numbers can be found relatively easy and be misused without any problems. From this point of view, the risk of "identity fraud" is accepted relatively willingly throughout society. Its acceptance is apparently economically cheaper than the improvement of the authentication measures would be. The question is how reliable an authentication and authorisation process has to be to void the claim that victims of "identity fraud" are to blame themselves.

"Identity fraud" in functional systems (economics, law, politics and science) happens, as described, through organisations. Organisations follow, as described above, a main emphasis, related to these functional systems. An example for this can be organised crime, which, as a rule, follows the economic primate (Lindlau 1987). The application of typical criminal motives (e.g. avarice, need for recognition, aspiration to power) certainly allows a detailed analysis of the social systems' vulnerability to the different types of identity fraud.

4.5.2 General theses on the appearance of "identity fraud"

On the basis of the categories and examples introduced in the previous sections, we can now develop theses on "identity fraud":

- Above all, "Identity fraud" is likely to consist of planned criminal actions (e.g. financially motivated in organisational systems), less often with actions that happened in the heat of the moment. Offenders are able, and required, to invest considerable resources (time, money, know-how) into the preparation of "identity fraud".
- The predominant types of "identity fraud" are those which allow both an authentication/authorisation and a reliable concealment of the deceiver's real identity (in the easiest way possible). These include mainly identity theft and deceitful identity creation.
- "Identity fraud" mainly find its victims where *weak authentication procedures combined with valuable or strong authorisations* are deployed. Particularly vulnerable in this case are interactions in social systems in which authentication takes place for roles only. Identification of a person is always vulnerable when it is not, or only insufficiently, supported by technology in electronic communication.

These theses correspond to the data on "identity fraud" published in current US-American and British studies[90], which examine the topic mainly on the basis of criminal acts following "identity fraud", and the motives of the perpetrators. This approach is made clear e.g. in the executive summary of the study by the British Cabinet Office: "ID fraud is an important and growing problem linked to organised crime in a number of forms: illegal immigration (including human trafficking); money laundering and drug running; and financial fraud against government and the private sector."[91]

The majority of the recommendations[92] on the prevention of identity fraud or on proposed reactions to identity theft published in the mentioned studies, as well as for the citizen mainly in the USA, are not far-reaching enough from a sociological perspective. The general recommendations relate to handling particular identifiers, how to behave when detecting "identity fraud", and recommendations, proposed legislation and regulation on the massive collection and evaluation of data on identity usage (e.g. opening of an account (Gordon and Willox 2003), "identity fraudsters"[93] and cases of deceit by use of these identifiers[94]. Structural improvements in the interaction in social systems, such as a broader introduction or usage of effective and socially integrated authentication procedures, are only superficially examined (i.e. case-related, e.g. to particular types of document or the opening of bank accounts).

4.5.3 The transition from identity collision to "identity fraud"

Although "identity fraud" is generally not to be expected in relation with identity collision, there is a creeping transition. If an identity collision occurs, is detected at least by one participant of the communication and taken into account deliberately, but not communicated, the transition to "identity fraud" is made. From this point of view, "identity fraud" includes identity collision that has become reflexive. The example of the friend and the car dealer, who act with different expectations, can certainly not be described as deceit. It is, however, of special interest because a possible "deceit" is not single-sided but the two involved persons try to use the situation to their own benefit, possibly for cheating each other. Both participants of the communication in this case know that they are taking two different roles within the

---

90 For example: Economic and Domestic Secretariat of the Cabinet Office, *Identity Fraud: A Study;* London 2002.

91 Ibid p. 6.

92 For example: http://www.privacyrights.org/fs/fs17-it.htm
http://www.dmv.ca.gov/pubs/brochures/fast_facts/ffdl25.htm
http://www.metlife.com/Applications/Corporate/WPS/CDA/PageGenerator/0,1674,P1516,00.html
http://www.cifas.org.uk/

93 Ibid p. 26

94 Economic and Domestic Secretariat of the Cabinet Office, *Identity Fraud: A Study;* p. 5, London 2002.

communication and they have to assume the same situation for their communicational partners.

The types of social system introduced earlier helps us to understand the transition from identity collision to "identity fraud". The transition from identity collision to "identity fraud" is possible if the parties involved participate in the same (and multiple) types of social system. This transition can particularly be observed with role collisions in interactional and organisational systems. There can be collisions of sets of expectations that are oriented differently concerning e.g. friendship, relations, neighbourhood, ethnics, shared philosophical or political opinions, or professionalism. Furthermore, there may be the transition from identity collision to "identity fraud" in terms of, for instance, a friendly, family or political relationship dominating a professional one. The persons involved interact in a way that appears to fulfil the expectations towards other members of the organisation, while the actually mutually evade them for their own personal benefit.

However, more important than this working-party phenomenon, which also arises in cross-organisation issues, is the interaction of members of an organisation with the organisation's clients. Even if a seller simulates interest in the client and not primarily at the sale, the participants simply have to assume that both sides aim to maximise their benefits and take part in a communication that is highly standardised and secures expectations. Determining whether fraud is at hand or not requires a precise examination and analysis of the social systems, the roles of the participants therein and observable actions in the light of possible motives. Legislation has developed a set of tools how this can be done.

4.6 Incidence of Identity Theft and Identity Fraud in Society

The value of online identification data (such as unique identifiers, login names and password codes) is a consequence of the increasing availability of services that depend on such data. Since these services are still fairly new and are still struggling to become accepted by the general public, abuses of identification data are also a fairly recent phenomenon. For this reason, identity crime is not a domain that is very commonly studied at this point. The dark number problem further increases the difficulty in obtaining reliable numbers. For example, complaints in the banking sector will typically be reported to the bank first, who has a large vested interest in keeping any problems out of official statistics by settling them privately. After all, if too many complaints are reported, potential users will be less likely to confide in the existing infrastructure, which would harm business growth.

As a consequence, reliable incidence data is extremely rare, and tends to be focused on the United States, where the problem of identity theft has been studied for a longer period of time. Many reports on ID-related crimes pertain to report numbers on ID theft, while in fact these numbers most often represent data on ID fraud. As we have discussed in section 2.1, identity theft is best seen as the misappropriation of an identity. The 'stolen' identity can, but often is

not, used for further offences; ID theft is a breeder offence. The acquired identity can be used for a wide range of crimes, such as drugs or arms trafficking, money laundering, but the most common type of crime linked to identity theft is identity fraud.

In 2005 a number of large scale ID thefts have surfaced, amongst others as a result of Californian legislation obliging companies and non-profit agencies to inform its residents if someone gained unauthorized access to their personal data. For instance, CardSystems, a credit card data processor, in June 2005 reported that 40 million credit card numbers were stolen from their database.[95] Online discount broker Ameritrade Holding Corp. in April 2005 admitted that about 200,000 current and former customers that a backup computer tape containing their personal information has been lost.[96] Bank of America reported the loss of backup tapes containing the financial records of 1.2 million federal employees. DSW lost 1.4 million credit card numbers and the names on those accounts, including information from shoppers in the Pittsburgh area, between November 2004 and February, to thieves.[97] Lexis-Nexis lost personal information of 280,000 people in their databases in April 2005.[98]

Not all of these stolen identity data will actually be used to commit further crimes. As far as we are aware of, no solid data exist with respect to the percentage of the stolen records that is used in further ID crimes.

With respect to the uses of the stolen identity in the US, the following numbers can be compiled from the various studies According to Elston and Stein, the US Federal Trade Commission reported 94.100 identity theft complaints between November 1999 and September 2001 (Elston and Stein 2002). The Privacy Rights Clearinghouse[99], another US organisation that collects data on the incidence of ID-theft, claimed that there were no less than 700.000 victims of identity theft in 2001 in the USA alone.

More recent FTC figures show a significant growth in number of consumer complaints about ID-theft (Table 4).

Year	**2002**	**2003**	**2004**
Information request	56779	108538	76926
Complaints	161896	215093	246570

Table 4. Identity theft records.[100]

[95] http://www.mastercardinternational.com/cgi-bin/newsroom.cgi?id=1038

[96] http://money.cnn.com/2005/04/19/technology/ameritrade/?cnn=yes

[97] http://pittsburghlive.com/x/tribune-review/trib/regional/s_326822.html

[98] ibid.

[99] For a list of their resources see: http://www.privacyrights.org/ar/idtheftsurveys.htm

[100] Source: FTC Survey (FTC, 2005)

The September 2003 Synovate report, prepared for the FTC, estimates the following numbers of ID theft victims:[101]

> "1.5 percent of survey participants reported that in the last year they had discovered that their personal information had been misused to open new credit accounts, take out new loans, or engage in other types of fraud, such as misuse of the victim's name and identifying information when someone is charged with a crime, when renting an apartment, or when obtaining medical care ("'New Accounts & Other Frauds' ID Theft"). This result suggests that almost 3.25 million Americans discovered that their personal information had been misused in this kind of fraud in the past year.
>
> 2.4 percent of survey participants reported misuse of their information in the last year that was limited to the misuse of one or more of their existing credit cards or credit card account numbers ("Misuse of Existing Credit Cards or Card Numbers"). 0.7 percent of participants reported misuse of one or more of their existing accounts other than credit cards – for example checking or savings accounts or telephone accounts ("Misuse of Existing Non-Credit Card Accounts or Account Numbers").1
>
> Including all types of ID Theft, a total of 4.6 percent of survey participants indicated that they had discovered they were victims of ID Theft in the past year. This result suggests that almost 10 million Americans have discovered that they were the victim of some form of ID Theft within the last year.
>
> percent of survey participants reported that they had discovered that they were victims of "New Accounts & Other Frauds" ID Theft during the previous 5 years. 6.0 percent said that they had discovered that they were victims of the "Misuse of Existing Credit Cards or Card Numbers," while 2.0 percent indicated that they were victims of the "Misuse of Existing Non-Credit Card Accounts or Account Numbers." In total, 12.7 percent of survey participants reported that they had discovered the misuse of their personal information within the last 5 years."

[101] http://www.ftc.gov/os/2003/09/synovatereport.pdf

Incidence of ID Theft in the Last Year, By Type of Misuse[102]	
New Accounts & Other Fraud	1,5%
Misuse of Existing Non-Credit Card Account or Account Number	0,7%
Misuse of Existing Credit Card or Credit Card Number	2,4%
Total victims	4,6%
Discovered That You Were a Victim in the Last Five Years	
New Accounts and Other Fraud	4,7%
Misuse of Existing Non-Credit Card Account or Account Number	2,0%
Misuse of Existing Credit Card or Credit Card Number	6,0%
Total victims	12,7%

Table 5. Incidence of ID theft as reported in the Synovate 2003 study for the FTC.

A more detailed breakdown of the uses of misappropriated identity data is provided in the FTC's 2004 annual report.

Type of fraudulent reuse	**Year 2004**
Credit Card Fraud	28%
Phone or Utilities Fraud	19%
Bank fraud	18%
Employment-related fraud	13%
Government Documents or Benefits Fraud	8%
Attempted Identity theft	6%
Loan Fraud	5%

[102] Each victim is classified as belonging to only one of the categories of ID Theft based on the most serious problem reported. Approximately 65 percent of those who experienced "New Accounts & Other Frauds" ID Theft within the last five years also experienced the misuse of an existing credit card or other account – 22 percent experienced the misuse of an existing credit card, 26 percent experienced the misuse of an existing non-credit card account, and 16 percent experienced both the misuse of existing credit cards and the misuse of existing non-credit card accounts. (The numbers do not add to 65 due to rounding.) Similarly, 40 percent of victims in the "Misuse of Existing Non-Credit Card Account or Account Number" category also experienced the misuse of an existing credit card account.

Type of fraudulent reuse	Year 2004
Other identity theft purposes, such as e-mail, medical, house rental, insurance, etc.	22%

NB: percentages sum up to more than 100% because some victims report more than one type of fraudulent reuse.

Table 6. Fraudulent reuses of identity information in the US in 2004.[103]

From a financial perspective, Visa and Mastercard (who represent some 75% of the general purpose credit card market) claimed a total loss to identity theft of 114,3 million US$ (roughly 88,9 million €) in 2000.

It is difficult to find reliable European figures. The UK Cabinet Office ID fraud study estimates the annual cost of ID fraud in the UK at £1.3 billion. A breakdown of the estimates suggests that the primary areas are: VAT 215 m£, money laundering 395 £m, credit cards 370 m£, insurance companies 250 m£, fraud reported to CIFAS a UK based credit industry fraud prevention association m£62.5. An interesting point to note on the basis of the UK Cabinet Office figures is that these numbers suggest the prime areas to be Customs related in the public sector and credit cards and insurance fraud in the private sector. However, this is primarily due to the fact that no figures are available with respect to social security fraud and work related fraud (e.g. working permits).

In line with US trends, also in the UK the number of ID fraud cases appears to rise. It is the fastest growing type of fraud in the UK; identity fraud is regarded as the biggest fraud problem facing society. CIFAS, for instance, claimed in January 2005 that identity theft rose by 600% between 1999 and 2004.[104] More generally, identity fraud is an international concern and an increasing threat, e.g. also in Australia it is the fastest growing type of crime[105]. The international perspective reveals that identity fraud crosses boundaries. The emergence of financial customer service centres in developing countries to serve European customers will have new implications for identity fraud.

4.6.1 Corporate Identity Theft and Fraud

Reports in the press about identity theft commonly focus on the individual. An equally significant type of identity theft and fraud involves companies. 'Long firm fraud' is one example of corporate identity fraud where a fraudster creates a company trading history

---

103 Source: (FTC, 2005)

104 See www.cifas.org.uk

105 According to the Australian Institute of Criminology, the estimated cost of fraud to Australia is in excess of $5 billion a year, which represents almost a third of the total cost of crime in Australia ($19 billion). http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/08ACDBBA372ED89DCA256ECF0007C146

allowing them to conduct transactions and then disappear. Another kind of corporate identity fraud is company cloning. Here a company's identity is used to perform new transactions (not necessarily fraudulent) and/or provide new services reusing the reputation of the company.[106]

Yet another type of corporate identity fraud specifically targets companies that do not take credit card payments. Fraudsters set up an account with a merchant payment service under the name of the company. Once the account is established, it can be used to harvest stolen credit card numbers. The fraudsters make payments to the newly established account, siphon the funds on this account off into their own bank accounts, and vanish. The genuine company is then saddled with the consequences of this scam, as the merchant payment service will hold it, at least initially, accountable for the fraudulent credit card transfers.

These kinds of corporate identity fraud can harm companies in multiple ways, including financial loss, damage to reputation, loss of actual and potential customers, industrial sabotage and industrial espionage leading to loss of competitive advantage and revenues.

Individual identity fraud for the purpose of defrauding a company

Identity fraud may be used by employees who apply under a false or stolen identity for a job and use their insider position to defraud the company. It may also be used by clients or suppliers that work with company. Individuals for example may combine long firm fraud, mentioned previously, with identity theft of another individual (e.g. a director of another company), in order to create a company with a forged background and history, which can then be used to defraud yet another company.

Corporate identity fraud for the purpose of defrauding an individual

The best known example in this category is phishing which was described in detail in section 2.3.1. In these types of scams, fraudsters use emails and fraudulent websites that hijack the brand of a well-known company (in 70-80% of cases these are financial companies).[107] This is essentially 'stealing' the company's identity in order to fool individuals into divulging information such as passwords or bank account details. It is estimated that up to 5% of recipients respond to such emails.[108] Another example is the case of companies selling bad medicine using the name of real companies producing these medicines.

4.7 Social and Economic Aspects

Identity theft entails several repercussions for victims. On the one hand, there usually is direct financial loss, the total amount can varies between some hundred dollars (or euros) to ten

---

[106] See case of Japan Tobacco International against 'JTI' http://www.tobacco.org/articles/country/monaco/

[107] Citibank and eBay are frequently used in the US. In the Netherlands the Postbank (www.postbank.nl) is a popular target.

[108] "Online banking: phishing for security" Deutsche Bank Research (2004) http://www.dbresearch.com/servlet/reweb2.ReWEB?rwkey=u142

thousands of dollars; all depend on the type of fraud performed by the criminal using the stolen identity information. The financial loss as a result of ID-related crimes is addressed in section 4.7.2. And on the other hand are the less tangible losses, such as the amount of time required to resolve problems, the damage to financial reputation, but also the trauma the identity theft itself incurs on its victims, the continual fear that new damage may arise even if the case appears to be closed. This kind of less, or intangible, loss can be described as the social aspect of ID-related crime.

4.7.1 Social Aspects

The social impact of identity theft and fraud can be regarded as a general cultural impact (Levi 2004) as it can occur to anybody. Some cases of ID-related crimes are clearly the result of victims being careless with their personal data, for instance, one can prevent becoming a spoofing victim as banks don't ask for the kind of data the spoofers asks his victims to disclose. Yet, even if the victim is extremely careful, identity theft can not be ruled out. Consider, for instance, cases such as the CardSystems case mentioned in section 4.6, where millions of credit card numbers where stolen from an organisation that should not have stored them in the first place. Not a single entity is to be blamed for ID-related crimes alone. Many entities, victims, payment merchants, internet providers, etc, all have responsibilities in preventing and fighting ID-related crimes. In cases of investigation, such responsibilities have to be identified.

In the online environment, the role of financial institutions in transactions has increased tremendously as many online payments consist of credit card transactions, which amount to changes in databases. This places new responsibilities on these financial institutions. Potter (2002) highlights the following new responsibilities:

- Providing a secure (integrity and confidentiality) process wherein financial transactions are completed
- Ensuring the privacy of account holders
- Ensuring the security of the accounts they own
- Ensuring that any financial activities are completed in accordance with the Uniform Commercial Code and Federal Reserve Bank regulations.

Also on the part of the (potential) victims, new responsibilities and liabilities emerge. The presumption of innocence makes way for a presumption of liability. In cases of criminal activity perpetrated with a stolen identity, victims have to prove their innocence (CIFAS 2004). This shift in the burden of proof is remarkable. The Canadian/American “identity theft” report even states that in some cases the victims have even been arrested and detained

by law enforcement authorities for a time before their true identity and relationship to the crimes could be established.[109]

The increase in numbers of identity-related crimes has leads to distrust in authentication procedures, especially from the viewpoint of clients and customers. Main reasons for this distrust are the lack of understanding of, and lack of control on, the technical authentication measures used in online transactions and the shift in the burden of proof in cases of identity misuse. Clients have to accept risks which they can't really calculate and influence.

To improve the trust within online transactions, trusted third parties have entered the market. This has, so far, not had the desired effects as it does not address the uncertainty and opacity of the online transactions. One example of this uncertainty is the implementations of PKI (Public Key Infrastructure) that uses Certificate Authorities (CAs). The chain of trust that should certify that a particular (encryption) key or message stems from an organisation that can be trusted is not very clear (question of the root of trust) (Ellison and Schneier 2000). Also, CAs are not responsible for the economic and social consequences of failed ore manipulated authentication. So, from the perspective of a client there is no reason to trust the trusted third party.

This negative cycle of distrust may get worse when new and stronger technical authentications are introduced and identity theft occurs again. Distrust in the system also increases as the result of the usage of personal identifiers as credentials or the usage in improper contexts. One example for this is the proof of age (are you over 18 years of age?) by requesting a credit card number. This leads to a proliferation of identity data in a context where these data are irrelevant.

Even in the case of properly functioning strong authentication, this fact has an influence on society. The implementation of security mechanisms such as logging and profiling procedures have to be paid for. Obviously it is the client or customer who bears the financial burden for authentication and authorisation mechanisms that increase security. But also other costs, such as loss of convenience, liberty, liberality and freedom are carried by the customers.

The financial loss and decrease in trust as a result of identity related crime on the one hand, and increasing costs for security, loss of convenience, liberty, liberality and freedom on the other hand, can be seen a societal balance that is controlled by authentication and authorisation. The balance increasingly seems to tilt in one direction. If the financial losses and corresponding decrease in trust reaches the point of social inacceptability, security is improved by means of tighter authentication, and a gradual loss of liberty, liberality and freedom is accepted. Reactions in the opposite direction, relaxing security measures in response to lower risks of identity-related crimes, can only be observed in rare cases. One

---

[109] http://www.psepc.gc.ca/publications/policing/identity_theft_f.asp
and http://www.psepc.gc.ca/prg/le/bs/report-en.asp#9

example is the abdication of the use of ID cards for personal authentication in Great Britain after the Second World War.

Not only tighter security measures have an impact on privacy, liberty, liberality and freedom. Identity crimes themselves, of course, also have a strong impact on these rights and freedoms. Identity theft is a serious threat against privacy as the culprit gains access to the private sphere of the victim by having access to her identity. The imposter is treated as if he were the victim and therefore can gain access to information that should only be available to the victim. Also other dimensions of privacy, such as dignity, autonomy, individuality and integrity are affected. When a victim's identity is stolen, the consequences of the impostor's actions may for instance deny a victim rights to funds, services, benefits, and even result in detention if the victim is wrongfully arrested.

This seems to result in an interesting tension: the need to protect privacy by protecting against identity theft and the need to partially surrender privacy in order to tackle identity theft. "To combat identity theft, business needs to verify the identity of applicants. To verify the identity requires access to personally identifiable information, but consumer unwillingness to provide that data contributes to the perpetuation of the crime." (Chapman 2004). Section 6.1.1 on countermeasures suggests ways in which this contradiction may be resolved.

One significant impact that affects virtually all victims is time loss (ITRC 2003). On average, the total active time spent by the victim to resolve a case is 607 hours. ITRC has reported a range of 2-11518 hours with the time spent sometimes extending over several years. Table 8 provides a breakdown of the loss of time for the types of identity thefts the US FTC defines.

Other intangible impacts include the emotional impact (e.g. a feeling of being defiled, stress, shame, helplessness, etc.) but also reputation damage (e.g. loss of creditworthiness). In extreme cases, the effects may include job loss, false allegations, criminal proceedings against the victim, public humiliation and a drawn-out procedure before the case can be resolved.[110]

4.7.2 Economic Aspects

The financial impact of identity-related crimes from the perspective of the victims can be decomposed into five types:

1. The economic cost most commonly measured or estimated is direct financial loss through identity fraud. The US Federal Trade Commission (Synovate, 2003) and a Report by the Gartner Group1 indicates that the damage of identity theft in the US amounts to around US $ 50 Billion in direct damage and an additional loss of approximately 300 million workhours for damage containment by the individuals. According to (Mitchison et al.,

[110] See for example http://www.bbc.co.uk/insideout/yorkslincs/series6/computer_doctor.shtml

2004) comparable statistics for Europe do not exist, but equal amounts are to be expected. Table 7 below gives different estimates for this figure from a range of sources.

Cost of fraud	Country	Type of fraud	Source	Year
1.3bn GBP per annum	UK	Detected identity fraud inc. credit card fraud data from APACS and CIFAS figures	UK Home Office (2002)	2002
1.6bn USD in 2002	Canada	Individual and corporate identity fraud	Identity Theft report presented to Canadian Ministry of Public Security and US Attorney General (2004)	2004
53bn USD in 12 months (02-03)	US	Individual and corporate identity fraud		

Table 7. Estimates of identity fraud in the UK, USA and Canada

The Synovate report provides some data on the costs of ID theft in the US in 2002.[111]

	new accounts & other frauds	misuse of existing accounts	all ID theft
loss to businesses, inc. financial institutions			
average per victim	$ 10.200	$2.100	$4.800
total	$32.9 billion	$14.0 billion	$47.6 billion
loss to victims			
average per victim	$1.180	$160	$500
total	$3.8 billion	$1.1 billion	$5.0 billion
hours victims spent resolving their problems			
average per victim	60 hours	15 hours	30 hours
total	194 million hours	100 million hours	297 million hours

Table 8. Costs of ID theft in 2002/2003.[112]

The sources for these figures stress that the numbers most likely under represent the true economic cost of identity fraud. Some costs are difficult to estimate exactly, or may occur years after the identity theft. Some costs are unreported, e.g. because companies do not want to damage their reputations with criminal proceedings, and some costs are undiscovered e.g. because they go unnoticed by victims.[113] For this reason the figures in the table above are best seen as a lower bound on the direct economic cost.

2. Identity theft, which as discussed in section 3.1.2, is not currently an offence in itself in most countries, is often a facilitating step (breeder offence) for criminal activity. In some cases identity theft may be a necessary step for another crime. The total 'cost' of identity-related crimes should therefore include the cost of the theft, as well as those of the costs of the crimes it breeds. The costs of identity fraud itself may include, for instance, the cost of preventive revocation of credit card numbers after they have been stolen, as in the CardSystems case to prevent misuse of them. The misuse itself would constitute ID fraud

[111] Ibid note 101.

[112] Source: http://www.ftc.gov/os/2003/09/synovatereport.pdf

[113] For an analytic framework showing the breakdown of economic costs, see 'Economic Cost of Fraud' written by NERA for the UK Home Office (2000)

costs. As noted previously, the numbers presented in the various studies usually do not make these distinctions.

3. Another type of indirect cost is the decrease in transaction volume due to a fear of identity fraud in online environments. Many consumers fear that their credit card details will be stolen and misused. This fear has, according to several surveys limited e-commerce growth (e.g. Ben-Ner and Putterman 2002). Though lost sales are very difficult to estimate, in the US alone the Federal Trade Commission reported an estimate of 2.8bn USD lost online retail sales for 1999. (Federal Trade Commission 2000).
4. Costs are incurred in order to detect identity fraud and they are subsequently incurred for investigation and prosecution of each case. It is estimated that an investigation requires 400 hours of work on average (CIFAS 2004). In this category we could include the costs incurred by individual victims in resolving a case of identity theft or fraud, as mentioned in the previous section.
5. A final indirect cost is the cost of improving security (of systems and processes) in order to fight against identity theft and fraud. This type of cost however contributes towards a reduction of identity theft and fraud in the future.

Investment motivation

To convince an organization (or better its management) to invest in better security, usually a business case reflecting the financial/business advantage has to be made. In this section we discuss how to motivate a company to take precautionary measures against ID-related crimes. Mitchison *et al.* (2004) assume that legislation is the most promising means as it would force all parties to comply. However, according to Zuccato (2004b), the urge for legal compliance is often not sufficient to convince enterprises to actually comply to the law. Legal compliance also depends on a company's (a) estimation of the chances of being caught when not complying, and (b) the weighing of the cost to comply to the legislation versus the cost of the potential loss.

In our view a holistic approach to determine whether or not to invest in better security. To this purpose, we propose to use an adapted form of requirement engineering that is made suitable for the ID-related crimes/privacy domain. This approach relies on the assumption that requirements are derived from the risk analysis, business modelling and stakeholder domain.

A view on risk analysis

According to DIN 31000 (DIN, 1979) a risk is defined in the following way: “A risk (r) consists of the expected likelihood of a hazardous event (p) and the expected damage (e) of it.” The expected damage is inflicted on an asset which, due to its own value, determines the amount of expected damage.

For an individual, her identity is the asset and its value is composed of the resources accessible through this identity. The asset, therefore, is a composite of values of other assets, given the likelihood that the asset can be accessed with the identity. Due to the "positive feedback" (Mitchison *et al.* 2004) of a successful committed ID abuse, we have to assume that the likelihoods are interdependent. We therefore have to assume conditional probabilities which imply that for value assessment we must use a Bayesian probability function. We have to make a simplification as the exponential runtime behaviour of Bayesian probability function make the practical application for a greater number of interdependent likelihood difficult. As a simplification we suggest to treat the assets as independent with the implication of dramatically reducing accuracy. This lack of accuracy needs to be compensated in the use of the results. When it comes to the organization to protect a customer/partner identity the determination of the asset and its value is not so straight forward. Various viewpoints need to be applied:

damage to the organization's reputation

damage from reduced customer trust (which is necessary to conduct business)

damage due to the fraudulent abuse of stolen identities

damage from legal prosecutions (Zuccato 2004b)

By considering potential damage from a general perspective, it is possible to avert the asset approach and move towards a baseline approach. This makes the approach fit the requirement engineering approach proposed below.

Requirement engineering

To understand what protection requirements are necessary on a system to prevent ID-related crimes, the problem can be approached from an insurance and a business enabler perspective. The insurance perspective is usually covered by assessing the risk reduction that can be achieved by an investment.

The FTC and Mitchison *et al*. (2004) indicated that customers are reluctant to use e-commerce because they are afraid of ID Theft. We assume that if this reluctance can be overcome, this would open new markets, and hence generate business benefits. This argument is supported by claims in the privacy debate by Frosch-Wilke (2001), Wright (1994), and Cate and Staten (1999) who say that its availability has the capabilities to improve customer retention, customer profitability and customer acquisition. These observations for privacy apply, in our view, to ID-related crimes as well, as the types of fear and lack of trust has similar grounds.

To foster both perspectives, a holistic requirement engineering approach which takes them into account, is necessary. In (Zuccato, 2004a) a process to elucidate holistic security requirements, is proposed, see Figure 5.

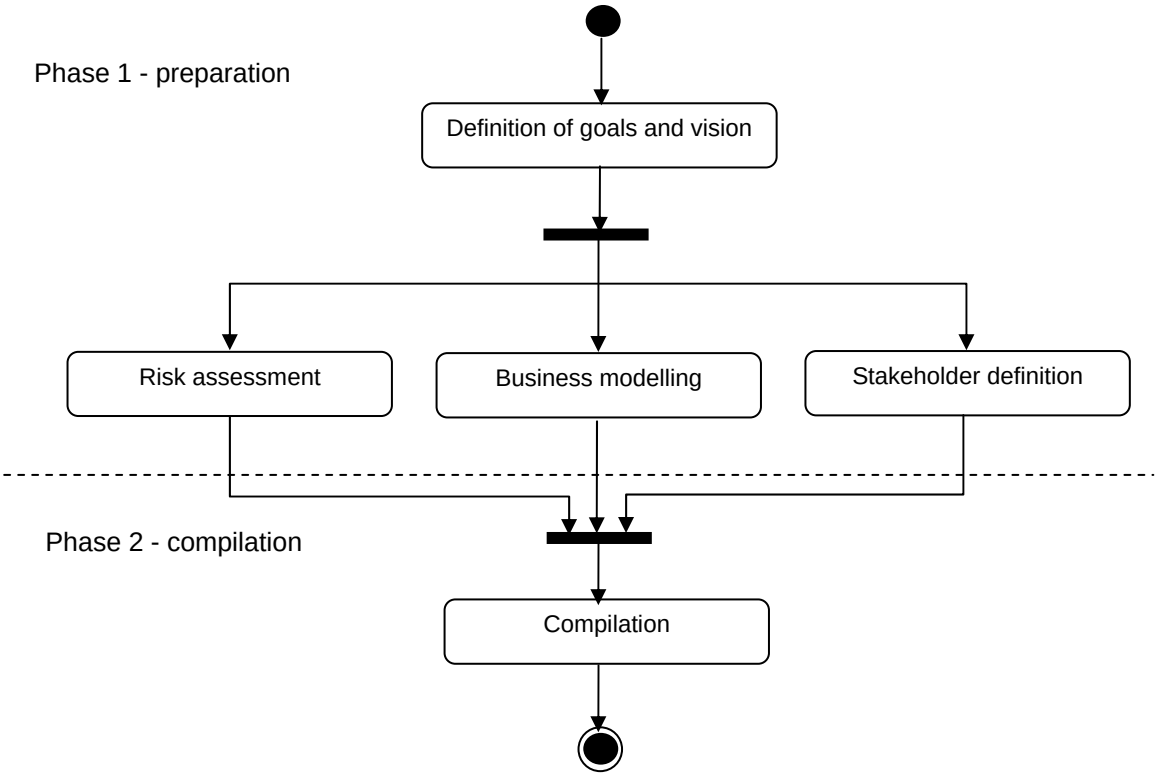


Figure 5. Requirement engineering process

This process argues that it is necessary to elicit requirements from three foci: internal, external and the risk analysis described above. The traditional process of eliciting requirements can be adopted to suit our purpose as follows.

The internal focus, with an emphasis on business, has to modify and enable the business process for ID Theft protection. This means that in the business process the need for personal information, and where it must be processed, has to be identified. The business units which have such a demand include Customer Relation Management (needs personal information to serve better), Marketing (want personal information to conduct direct marketing) and Security, Audit and Control (wants to assign people to (malicious) actions). This identification of needs has to lead to a statement about the appropriate protection.

The second focus means taking external sources for ID Theft requirements into account. This enables a social and business treatment of the problem. According to Zuccato (2004a) this approach relies on stakeholders. For ID Theft, this could mean (non-exclusively) Individual Customers, Customer Protection Organizations, Privacy Protection Organizations, the

Legislature and Law Enforcement as important stakeholders. Except for the customer and the legislative stakeholder, we suggest workshops as the primary means to elucidate the external requirements. For the customer, we suggest interviews and surveys as the primary means, and for the law and legislature, we propose literature research. Those approaches are described in Zuccato (2004a).

Concerning risk analysis, the third and last focus area, we suggest using the risk analysis approach presented above. Due to its simple and baseline like character this approach is suitable within a privacy requirement engineering scenario. In respect to the second phase, compilation and prototype, (Zuccato 2004a) assumes no difference between security and privacy requirement engineering.

Difficulties in countering identity fraud

There are several economic reasons why identity theft and fraud are difficult to tackle. One problem is the moral hazard in the securing of identity information. For instance, perverse incentives arise when the party that is in a position to protect a system is not the one who suffers the consequences from a security failure (Anderson 2001). There are several examples of this in the field of identity-related crimes. For example, many credit card companies and banks will reimburse consumers for fraudulent transactions, provided the consumer has taken certain elementary precautions. The cost of this kind of fraud resolution is passed back to the consumer indirectly, in the form of higher service charges for companies (shops), who of course pass these charges on to the customers through higher prices for their goods and services. There is no direct cost to the consumer, and hence no direct incentive to take every possible measure against information theft.

Moral hazard can also be seen on the part of companies that send out pre-completed application forms for bank accounts or credit cards to home addresses of their (prospective) customers. Junk mail such as this is a common source of personal information for identity thieves[114] but the disastrous consequences fall on the individual, rather than the company responsible for creating the opportunity for ID theft and ID fraud. A similar example is the recent case of a nationwide identity theft in the US. Commercial information companies inadvertently sold personal data, including social security numbers, to impostors posing as business officials.[115] Though the onus should have been on the companies to carry out more background checks on their clients before selling the personal information, in practice there was little incentive to do so. So, again, the burden of the cost rests not on the shoulders of the origin of misuse, but on the innocent victims.

[114] http://uk.biz.yahoo.com/moneyweekly/identitytheft.html
[115] http://www.washingtonpost.com/wp-dyn/articles/A40379-2005Feb20.html

A second problem arises from the disparity between people's stated concern for the privacy of their personal details and the level of action they will take in order to ensure it. Acquisti (2002) points out that the negative utility which may occur as a result of identity theft is almost impossible to calculate. Potential outcomes could be catastrophic for an individual (losing one's job, criminal prosecution, etc.), but the probabilities of these events are low. Furthermore, individuals tend to place an increasing discount rate on risks the further they occur in the future Rabin and O'Donoghue, (2000). This implies a myopic outlook and a bias for present gratification. Therefore, a paternalistic rationale for intervention exists: individuals do not take the precautions they would take if they were able to rationally estimate the negative utility of failing to secure their personal information.

A third, and novel, challenge is posed by the spread of digital communications. The same benefits that make the Internet attractive to individuals and companies alike, namely the speed and efficiency of communications and transactions, also make it a valuable tool for identity thieves. Phishing emails provide a good example. It is possible that individuals who give away their banking details to a spoofed website would similarly respond to a fraudulent phone call or letter. Yet, cold-calling large numbers of people is prohibitively expensive for potential fraudsters. Also, phone calls are easier to trace. On the internet, even a very low response rate to phishing scams (up to 5%[116]) is an economically efficient way of targeting potential victims. The marginal cost of sending an email is next to zero and the potential gains if the victim responds are high.

Electronic media also enable scams to be set up inexpensively with basic technical knowledge. Many consumers have become accustomed to Internet shopping and will hand over payment details with relative ease. A professional-looking website can be set up by a single individual and can reach people worldwide. The ease with which a website can be set up also assists fraudsters in corporate identity theft, e.g. by using a similar domain name and imitating a genuine company's site. The examples of corporate identity theft described earlier bear testament to this.

It is undesirable to greatly limit the benefits of an increasingly networked world in order to prevent theft and fraud. Yet, policy makers do have a role in ensuring that proper incentives exist for companies that collect and hold personal data on individuals to safeguard it well. General countermeasures against ID-related crimes are discussed further in chapter 6.

---

[116] "Online banking: phishing for security" Deutsche Bank Research (2004) http://www.dbresearch.com/servlet/reweb2.ReWEB?rwkey=u142

4.8 Conclusion

In many countries, identity fraud is the fastest growing type of fraud, and in some it is even the fastest growing type of crime. Identity theft, though not at present a crime in itself, is a breeder offence which usually leads to other criminal activity. Many of the impacts of identity theft affect both individuals and companies. Victims may suffer financial loss, damage to reputation and loss of credit rating leading to denial of loans. Many hours may be spent trying to undo the damage, and in some cases the effects may not be reversible. In extreme cases, identity theft has led to individuals being wrongfully arrested and prosecuted. Everyone is susceptible to identity theft and it therefore has a widespread social impact.

Economic costs extend well beyond the reported figures. Other costs identified include the unreported and undiscovered financial losses, the damage to consumer confidence in online transactions and therefore the loss of potential business, the cost of crimes other than identity fraud perpetrated on the basis of identity theft, the cost of discovery and investigation and the cost of resolving the problems created by the theft or fraud. There are a number of reasons why identity theft is a challenging problem to tackle. In some cases there is a lack of incentives for the parties in possession of identity data to secure the data adequately. From an individual perspective, there is a lack of awareness about the negative utility that can arise from identity theft. The Internet and the increasing importance of electronic transactions exacerbate the problem as it becomes easier for an identity thief to carry out fraud.

5 Technical Aspects

5.1 Introduction

As discussed in the previous chapter, authentication and authorisation are crucial processes for ID fraudsters as they play a key role in establishing trust that can consequently be misused for criminal purposes. Chapter four focussed on the social aspects of authentication and authorisation. Technical authentication and authorisation procedures thus are the Achilles heels of information and communication systems.

In general, identity theft is likely to be feared in cases where powerful authorisations are used together with weak authentications. For example, identity theft becomes more attractive to the thief if a stolen identifier has multiple purposes. One example of this is the social security number, or the driving license number, that is used as the de facto ID standard in the US. These numbers are particularly valuable for prospective culprits. The same rule applies to integration of authentication and authorisation procedures in technical systems by using single sign on (SSO).

Further problems arise from the use of internal verification patterns in authentication procedures. One example was the verification procedure of credit card numbers which was used until 2001 by an algorithm that takes name as additional inputs. When the credit card was used to pay via the Internet the internal verification of the submitted credit card number in these days was often done automatically by the online shop system against the submitted name. Once the verification algorithm was known, anyone could generate faked credit card numbers (identity creation)[117] and got them verified easily when using them via the Internet.[118] As described above, the fraudulent creation and use of a credit card number that already exists turns into identity theft. The verification procedure has been changed since and now relies on additional random verification numbers, such as the three digit SVC number on the back of MasterCards.

A principal cause for the increase in ID-related crimes in the online world is the fact that authentication procedures here are intrinsically less secure than those in the offline world. When moving a system from offline to online, often the technical authentication procedures is adapted to the online capabilities, frequently without adapting the security measures. For instance, instead of relying on a "physical credit card", which requires possession, the online process relies on "submitting a number". The offline procedure allows for more security

---

[117] For example by using this credit card number generators such as http://www.elfqrin.com/hacklab/pages/discard.php

[118] See for example: http://www.computerbetrug.de/kreditkarten-white_plastic.php?p=17%25257C106%25257C and http://www.meister-it-service.com/sicherheit_b3.htm

checks to be performed than the online procedure that it replaces. Another problem is that the explicit procedures usually are transformed to the online world, but the implicit procedures and contextual cues are not. Security and trustworthiness therefore often decrease. The frequent phishing cases involving online banking sites reported in the media are an example here. The authentication of the actual site may be adequate, but if people are incapable of establishing the trustworthiness of the site they are lured to, this does not help.

Another major problem often seen is unrealistic trust in technology and security of complex systems. In many cases, a user, from his perspective, trusts one component used for a special purpose, but does not oversee the complex nature of the system and the multiple purposes it has or could be used for. As a result, the security of the system is constantly under threat, for example because users do not install updates or patches which are necessary for the system as a whole, but not for the user's limited view on the system. Such weaknesses can then be used to steal authentication data and thus to prepare identity theft. Possible targets are:

- Hardware and operating systems including drivers (PCs, PDAs, ID cards etc.)
- Applications such as mail clients, browsers etc.
- Electronic communication (Chat, eMail, www)

The current chapter addresses ID-related crimes from a technical perspective. It first describes common methods of (technical) attacks against authentication procedures and analyses the associated vulnerabilities, both with respect to the identity of persons and with respect to the identity of IT systems. Next, two scenarios are sketched more in detail focusing on attacks against biometrics.

5.1.1 Authentication of a person by an IT system

Authentication of persons is primarily related to the verification of the identity of an individual for the purpose of controlling access to restricted resources or areas. This process is regarded to be the gatekeeper, as well as the “Achilles heel” of the security of a system. Authentication is mainly based on something someone **possesses**, such as an identity card, a passport, a smart card, something one **knows**, for instance a password, a PIN, an answer to a question, or something one **is**, their human characteristics (physiological or behavioural). The main advantage of the first two ways of authentication is the fact that they are inexpensive, simple to set up, and user-friendly. Moreover, both a password and a smart card can be easily replaced in case they are lost. Most systems using these methods of authentication will also “lock” the associated accounts in the case of loss of the key, which will also happen in the case a password or PIN is incorrectly entered several times. Nevertheless, smart cards or passwords can be easily lost, stolen or shared, and thus a high level of security is not offered. As pure knowledge-based or pure possession-based authentication processes are not very strong, usually the two methods are combined. An example is the all familiar ATM, which

uses a two-factor authentication requiring not only a user PIN (something you know), but also a physical card (something you possess).

From a technical viewpoint, an identity is just a digital pseudonym that represents a person. So, there must be measures to prove that the digital pseudonym actually belongs to the person who claims it does.

Such a technology should ensure the following properties:

- A person can use its own digital pseudonym without restriction;
- Another person cannot use this digital pseudonym.

There are different technologies aiming at this goal, but with a certain probability of failure. When a pseudonym is used, it must always be in connection with proof that it was used by the person to whom it belongs.

IT systems are able to recognize a human by (Pfitzmann 2005):

- what he is (by using biometric techniques);
- what he possesses, or;
- what he knows.

Figure 6 shows some examples of what can be used as proof for a particular pseudonym. Some of the proofs can also be applied to the process of recognition of humans by humans, for instance look, and voice. Hand geometry, retina patterns, magnet strip cards, chip cards and calculators do not play an important role here for obvious reasons. Of course, combinations are possible and useful, e.g. a passport combines "what you are" (appearance through a picture and partially unconscious actions through an autograph signature) with "What he has got" - the passport itself.

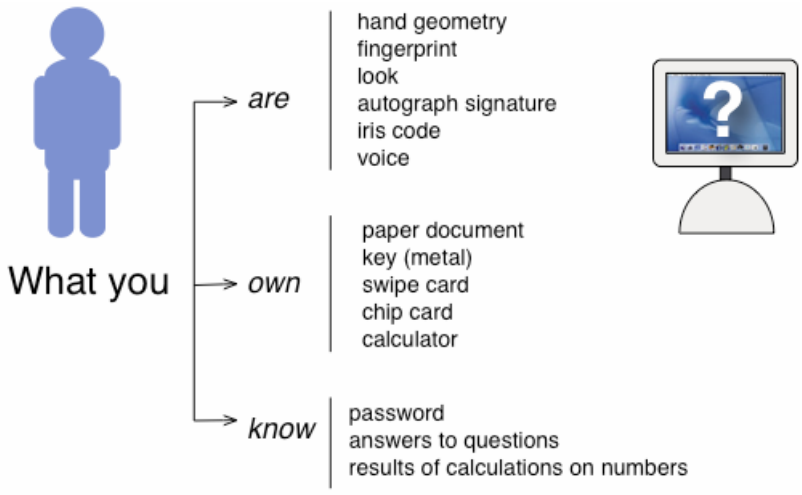


Figure 6. Authentication of a Human by an IT System.

The methods of proof can be decomposed further. Biometric proof, for instance, can be decomposed in product checking and process checking. Checking the validity of an autograph signature, for instance, can be taken to mean to "check the results of the signing process" (product) by comparing two static line patterns, but also as meaning to "analyse the dynamics of the signing process" (process), for instance by comparing pressure and acceleration values of signatures. Process checks are very suitable for behavioural biometrics, such as vocal patterns, typing patterns, gait analysis and the style of writing for pen inputs.

Within process checks, one furthermore has to decide whether the tests is to be performed just at the beginning of the process, at additional (fixed) time intervals or permanently. Some biometrics are suitable for permanent monitoring, for example key stroke monitoring that can run as a permanent background process thereby continuously confirming the presence of the authorised person, whereas other clearly only suitable for one-shot authentication: one cannot demand the subject to keep his hand permanently on the hand geometry scanner.

One-shot versus permanent authentication also plays a role in the other types of authentication. A metal key, or a USB dongle can be required to be present permanently during an interaction, but also only to unlock an application or access door.

Up to now, most authentication in the online world is carried out by means of the 'what you have' and 'what you know' methods. Both types of authentication means, as we have seen, are relatively easy to obtain which makes them relatively insecure. Biometrics are deemed more secure as they are more closely linked to the person. The iris never leaves the human body, for instance. Yet, also these methods of proof can be misused. We will turn to ways to spoof this kind of biometrics in section 5.2.2.1. In recent years, physiological biometrics have started to enter the marketplace in larger numbers. Fingerprint scanners are becoming affordable and already standard on some laptops, and also portable hard disks (such as the LaCie SAFE Mobile Hard Drive.

Experiments on human actions by psychologists and mathematicians have demonstrated that human behaviour can be predictable as far as it concerns repetitive tasks. In this way not only physiological but also behavioural human characteristics can provide valuable information for human authentication. The traits used by these methods are less susceptible to duplication or loss when compared to the traditional means of authentication, and even the physiological biometrics methods mentioned above. They are portable and may involve a non-contact authentication, yet use something integral to something the person is. The proper implementation of these systems prevents the sharing of secrets that could be used fraudulently. Therefore, we may expect to see more of authentication methods such as keystroke analysis and mouse gestures.

5.1.2 Authentication of an IT System by a Person

Most cases of ID fraud will involve using one or more of the means of authentication in the previous section to mislead an IT system into believing the culprit is mentioned is who he claims, to be. Yet, ID theft may involve tricking a human into believing that an IT system is what it claims to be in order to misappropriate ID data from this person. We therefore have to look into how a person authenticates an IT system

They can use:

- what the IT system **is**
- what it **knows**
- **where** it is located

Figure 7 gives some examples of specific measures.

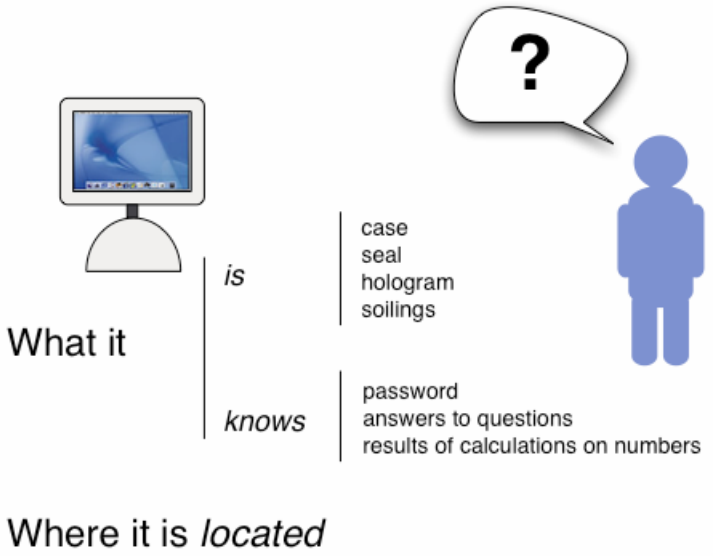


Figure 7. Authentication of an IT System by a Human.

Some of these are frequently used to establish the authenticity of the IT system. Consider, for instance the digital certificates used in SSH connections. The user can in principle verify the trust chain and establish that such a certificate is valid, notwithstanding the problems associated with the opaque CA system as mentioned in section 4.7.2.

An interesting proof for the authenticity of the IT system is the location. Usually we take it for granted that this indeed is a signal for the validity of the system. Yet, there are numerous cases where this assumption proves wrong. Dummy cash machines and magnetic swipe devices have been installed in front of a real ones, typically during weekends, covering them to the extend that users did not notice. The dummy machine initiates a transaction just like the valid machine would do, so it asks the personal identification number (PIN) for the inserted EC cash cards and stores it. Next, then system will display something along these lines: “Your

faulty EC cash card will be impounded, please contact your bank on Monday for assistance." Needless to say that the culprits then have both the physical EC card and the corresponding PIN, which can then be used to withdraw cash until the card is blocked by the bank on the victims request.

5.1.3 Methods to manipulate Authentication Procedures

The processes of authentication of a person by a system and the authentication of a system by a person can be described schematically as in Figure 8.

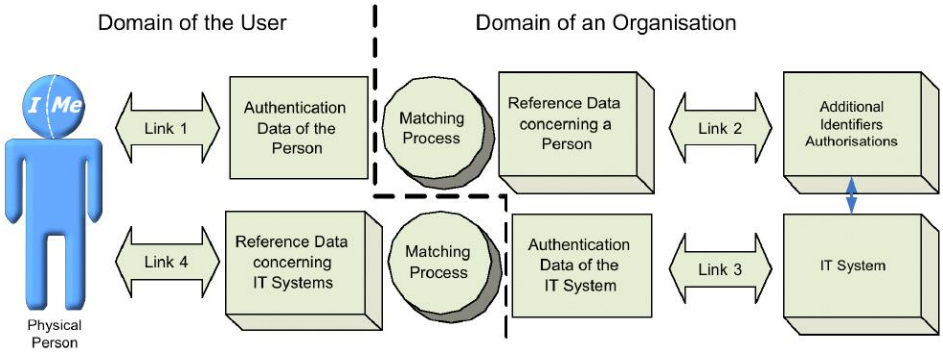


Figure 8. Authentication procedures between persons and IT Systems.

During the enrolment phase, which is not shown in the diagram, authentication of the subject is performed and reference data is generated. Link 1 describes the association of the subject with the authentication data that is either supplied by this subject (for instance a fingerprint in the case of biometrics). Additionally, other data may be collected to be used in later authentication processes. These data establishes links 1 and 2.

In addition the person is made familiar with the use of the system, and the location where it is placed. In rare cases, further authentication information and reference data to authenticate the system to the user is generated and the appropriate links 3 and 4 are established.

As introduced in section 4.4.2, identity changes and thus identity fraud base on rearrangements of identity linkage. So the links between a physical person and authentication data shown in Figure 8 is the target of an attacker, though the attack in some cases is not directly carried out against that link (indirect attack). Various currently discussed occurrences of identity fraud and identity theft can be categorised as follows:

- Identity Theft
    - Direct attack on the Link between the person and the authentication data (link 1, see Figure 8) using one or more steps
        - Worms installing for example a key logger
          Authentication data is directly taken from a person by manipulation of his

input device (in most cases local computer). This attack is directed non selective to many input devices (1 : n attack); the person is not addressed directly.

- Social engineering
  Using communication for example via telephone authentication data is directly taken from the user by giving him a seemingly plausible reason for disclosing the requested data e.g. for testing purposes by administrative personal of the enterprise's IT department. This type of attack is directed to a specific person.
- Trojan Horses / Key logging etc. sent via e-mail attachment
  In the first step a spam mail containing malicious code in an attachment is not specifically sent to various users (1 : n attack). By opening the attachment for example a key logger is installed that starts obtaining the authentication data in a second step.
- Spoofing of (biometric) sensors without co-operation of the person to which they were originally linked
  In the first step the needed biometric data such as a photo of the eyes is take from the person. In a second step, a printout of the photo is used to spoof for example an iris scanner. This type of attack is directed to a specific person.

o Indirect attack on reference data or via other links

- Readout of Person related identifiers, authorisations and reference data
  In this case the attack is directed to the centrally stored reference data and related additional identifiers. This attack can either be carried out against the whole database (1 : n) or specific data records (1: 1).
- Manipulation of reference data concerning a person
  By manipulation of the reference data, the attacker is able to redirect link 1 to himself while the IT systems expects an authentication by the person the not manipulated reference data originally was linked.
- Phishing (3 Steps, indirect attack, 1:n)
  In the first step the attacker sends a spam mail that seems to originate from a trusted brand name (e.g. a bank) to many recipients (1 : n attack). This e-mail usually urges the recipients to click on an embedded link that leads them to a manipulated web site. This web site again has the layout of the trusted brand, so that the link between IT system and authentication data (link 3) is being attacked. On this site the user is duped to enter authentication data.

- "Man in the middle" attacks[119]; they allow for both forms of attacks
  In this type of attacks the communication between user and system is intercepted. This type of attacks is potentially very powerful and allows, among others (such as substitution attacks), for different types of identity theft:
    - Identity theft by readout of authentication data not securely communicated by the user (direct attack on link 1, 1 : 1 attack).
    - Replay Attacks
      An IP-packet containing authentication data is manipulated concerning the sender address and resent to the receiving system. This type of attack is directed to a user of a specific input device (direct attack on link 1, 1 : 1 attack).
    - Identity theft by redirecting the communication to a manipulated web site e.g. by using DNS-spoofing, manipulated proxies or manipulation of rooting tables. On the manipulated web site the user is duped to enter authentication data. This type of attack is concerning some steps similar to phishing (2 steps, indirect attack on link 3, 1 : n attack).
- Deceitful Identity delegation and deceitful identity exchange
  In this case the person co-operates with the attacker giving his authentication data deliberately to him with the knowledge that this data will be abused. The attack is directed towards link 1 and is directed 1 : 1 (deceitful identity delegation) or more complex in cases of deceitful identity exchange.
- Identity Creation
  In cases of identity creation, the attacker typically uses the enrolment phase to manipulate either link 1 or link 2 (see Figure 8) so that the chain from him as the physical person to the authorisation breaks. Thus he probably can abuse the IT system for a certain (and probably long) time.

5.2 Two scenarios for identity fraud with biometrics

In this section we describe two scenarios for ID fraud using biometrics. These are written from different technical perspectives. The first focuses on laboratory tests to illustrate some general technical implementations of identity theft (see section 5.1.3), comprising a situation that is not widespread at present, but one that is under study in numerous places as it provides a way to perform unobtrusive identification which makes it very suitable for public places and shopping malls. The second uses the perspective of forensic experiences with biometrics

[119] See for example: http://md.hudera.de/jura/rechtstatsachen/node31.html and http://en.wikipedia.org/wiki/Man_in_the_middle_attack

fraud. These scenarios suggest how the IDM system – biometrics – functions in different fields and can be approached differently in order to counter ID fraud.

5.2.1 Scenario 1: Attacking an authentication, identification and tracking system using physical biometrics

Suppose a system which performs real-time facial and/or body recognition and/or human tracking for surveillance, entertainment or commercial purposes. The digital identity in such a system, meaning the digital representation of a person, can be the digital representation of his face and/or body, a nickname, his height (if human tracking is performed as well). Given a single uncompressed or compressed colour image, the human detection/localization process aims at automatically and reliably identifying and determining all regions in the image which contain a human regardless of its three-dimensional position, orientation and lighting conditions. The human identification procedure uses human attributes extracted with the aid of face and body modelling, while the human tracking process aims at allowing cameras to "follow" the identified human under varying complicated conditions, such as occluded regions, abrupt motion, indoor/outdoor conditions, and varying illumination conditions.

The main specifications of such a system involve:

- the functionalities of the cameras – such as that cameras should continuously acquire images, they should share a common time code and their field of view should be known in advance;
- the division of the system into modules (human content detection and localization, human content identification, human content tracking, real-time controller, cameras, database) and sub-modules;
- the input and the output of each module (exchanged data);
- the interaction between the system modules (exchanged control messages).

For the sake of the scenario (experiment), such a system could be reduced to a simple indoor (for limited varying environmental conditions and background) testing area including a terminal and a camera for the registration phase and a corridor with 3 cameras. The registration phase includes the acquiring of the image of the person to be tracked as well as a nickname of their choice and their height (which will be used for the determination of the camera that is currently capturing images containing the person to be identified and tracked). After a person is enrolled into the system, the system will henceforth automatically identify and track him in the area that the cameras cover.

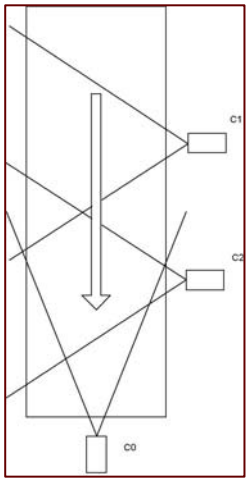


Figure 9. Testing area of the scenario: The field of view and the human's walking direction are depicted.

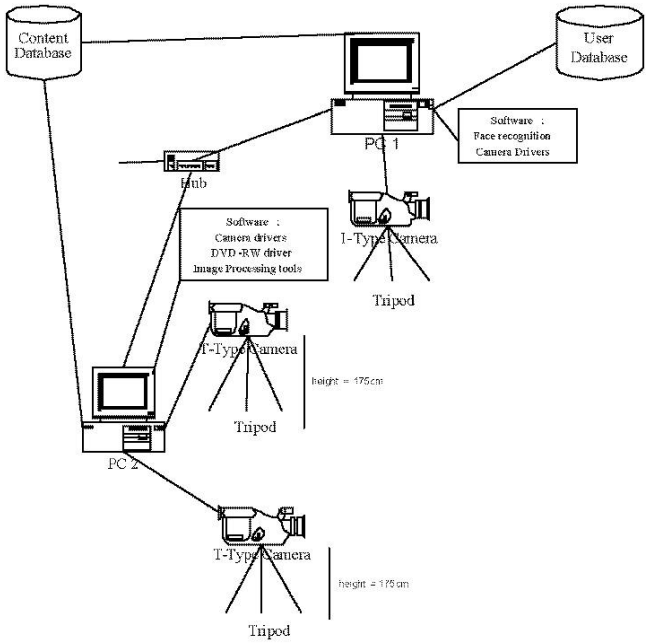


Figure 10. Hardware equipment of the scenario.

In this scenario, identity theft may take place either during registration to the system or during identification and tracking. The following cases of ID theft can be imagined in this setup.

One case is the provision of fake height information during registration which can lead to the inability of the system in tracking – but not in identifying – the person since this information is used by the system to measure the distance of the identified person from specific cameras and thus determine the camera that is currently tracking them. This vulnerability of the system can be overcome by the automatic calculation of this information by the system (automatic regulation of the height of the registration camera, etc.).

Another case is when a person disguises himself. The system will then have difficulties in identifying the subject if specific features of the person are changed (hair, facial colour, etc). However, since height plays such an important role in tracking people in the given system, if a person tries to disguise himself as another person who has been registered into the system, with a different height, then the identification process may provide a false positive, but the tracking process will not. In case of similar heights though, a person can mislead the system in two ways: the system will either (a) be unable to match the person with an image in its database, or (b) provide a false positive, by misidentifying the disguised person. Moreover in case the person during the enrolment phase (registration) wears sunglasses or has a beard, their facial features are not easily distinguished and thus identity fraud is more easily performed. These faults can be addressed. One solution is the segmentation into very small pieces of both the captured image of the person to be authenticated and the registered image and the emphasizing on the segments that bear strong similarity. This allows human identification with a remarkable reduction, but not elimination, of the false positives and the false negatives, even if the face is occluded due to sunglasses or a hat.

And what happens when only one camera is used for human authentication? The person could fool the system just by providing a photograph of the authorized user to the camera that performs authentication. Aiming at making the system more robust, more cameras could be used during the authentication phase (acquiring both frontal and side views of the person's face) and thus more than one facial images of the person should be captured and processed during the enrolment phase, or texture information could be used during face detection, but still without eliminating the danger of id fraud. The combination of facial recognition with another means of authentication (PIN, smart card, etc) could even further reduce the success of an id fraud effort.

Another case leading to a false positive, which is very difficult to deal with, is that of identical twins. This system vulnerability – based on its difficulty to distinguish between the twins- could be exploited by one of the twins who may choose to use the identity of the other.

Such a system could be also used when the registered people are those who should not be authorized to system. In such a case, the system is much more vulnerable to id fraud attack, since it is easier for a person to be not themselves than to be someone else! Id fraud can then take place through the growth of beard on the person's face combined with sunglasses, the covering of a part of the face (pretence of a recent accident) or through surgery. Taking into account the fact that face recognition is a non-contact authentication technology (since images can be captured even from a distance), user authorization can be performed even without the person's notice by identifying the registered non-authorized people. Frequent updates of the systems database could improve the system's robustness and reliability, whereas amelioration of the authentication process could be attained through the capturing of body images as well, so that authentication requires both face and body features match. In long term applications,

however, the frequent updates of the person's records in the system are compelling, since human body features change more easily.

Of course, the system actual vulnerabilities and counter measures depend on the system's application domain. Entertainment, security and government, require different levels of reliability and face different likelihoods of attacks. For instance, installation of this kind of system in an amusement park, will probably not run the risk of serious attacks, whereas terrorists may pose a serious threat in trying to undermine the same kind of system in an airport.

5.2.2 Scenario 2: Possibilities of Identity theft with biometric devices

Over the past few decades, both industry and governments have shown a growing interest in biometric devices. Terrorism has highlighted the need for better identification systems for people as well as for improved systems for controlling access to buildings and countries. Another reason for investment in Research and Development in biometric devices is the massive growth in internet-based systems – whether for e-commerce, e-government or internal processes within organizations. As described earlier, biometrics offer a way to increase the security of authentication systems by complementing single method (what you know) and even dual methods (what you know and what you have) with the third type of identifier, what you are.

Biometric systems (especially fingerprint scanners) are mass market products at low cost, and can easily be integrated in consumer electronics, like PDA's. Fingerprint scanners are appearing in more and more products (keyboards, mouse, plug in device, USB stick, and even hard disks). Systems using fingerprints, iris, hand scans, and faces are commercially available and routinely used at e.g. airports. Commercial interest in biometric systems has grown rapidly in 2003 and 2004. If we look at the patent applications, the number of applications with the word "biometric" has grown from twenty per year in 2002, to thousands per year in 2003 and 2004.

With conventional security systems, users may suffer from socially engineered attacks, as can be seen from the growing number of cases with fraud at ATM-machines. Biometric devices may provide a solution for this kind of crime, but biometric devices still can be 'spoofed'. The manufacturers of biometric systems are becoming more aware of the problems with tampering, and solutions are provided how to avoid the possibilities to tamper with their systems. Some patent applications describe ways of detecting if persons are alive and if someone tampers with the systems.

In the next sections we describe some of the ways of tampering with biometric device for the purpose of ID-related crimes.

5.2.2.1 Spoofing

The spoofing of biometric devices by making copies with silicon or any other casting material of the fingerprint is legendary. The first publications on spoofing were from the Yokohama National University in Japan (Matsumoto 2002), which even gives a detailed recipe, and from T. van der Putte (2000). Another publication that attracted a lot of attention was CT Magazine (Thalheim and Krissler 2002), a popular German computer journal.

Experiments with spoofing

The Dutch Forensic Institute has done extensive tests with the various biometric systems. Several fingerprint systems and an iris system have been tested for possibilities of tampering. In most case it appeared to be easy if a person allowed to enrol into the system is cooperating. Some biometric features can also be copied without this person's awareness and consent (for example fingerprints taken from a glass.

A low cost (Panasonic) iris scanner in our laboratory could easily be faked with a photograph of a person revealing the iris (Figure 11). Punching a hole in the place of the iris turned out to be sufficient to mimic the light absorption exhibited by a real iris and fool the system into falsely accepting the photo as a real iris. It is claimed that high end scanners do not have this disadvantage:

> "Because the iris and eyelid vibrate at known frequencies, and because oxygenated tissue reflects light at a specific frequency, it is possible to differentiate between a real person and a digital image, glass eye or contact lenses with irises printed on them."[120]

We have not substantiated this claim.

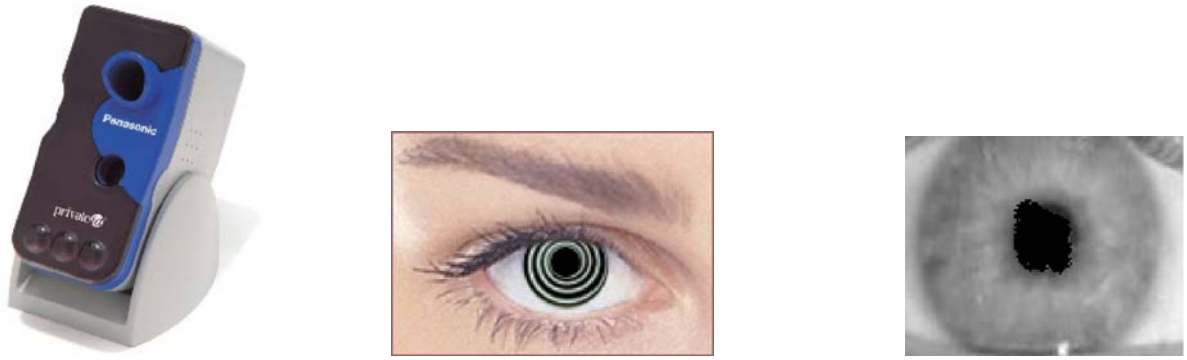


Figure 11. Image of iris spoofed by low resolution print and also possibilities with fun lenses for enrolment and access control

[120] http://www.csc.com/features/2004/45.shtml

Figure 12. Silicon casts of fingerprints with silicon cast negative and acrylate paint as positive.

The NFI lab has also tested the methods described in literature to create copies of fingerprints. Figure 12 shows the use of Silmark silicon casting material to copy a fingerprint. The negative can then be used to create a positive made up of a thin layer of acrylate paint that can be used as a layer on top of one's finger to impersonate the victim whose fingerprint was acquired.

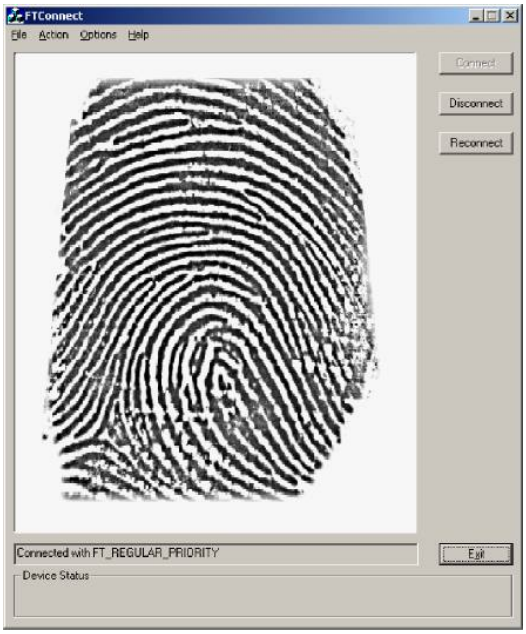


Figure 13. Fingerprint access with copy of fingerprint on scanner "Digital Persona".

The method described uses a mold created from the actual fingerprint. This means the victim has to cooperate in the identity change (identity takeover or identity delegation).

The literature (e.g. van der Putte and Keuning 2000) also describes methods to use photographs of fingerprints left on glasses to create the required positives by means of photolithographic processes. An even easier method is reported by the Computer Chaos Club[121] which relies on a fingerprint on glass, simple means such as superglue, wood glue, a digital camera, an overhead foil and a laserprinter.

Several patents and information sources describe the method of computing a template to be used for the comparison. Depending on the implementation, it may be possible to reverse engineer the template to create a 'biometric feature' that, when presented to the scanner matches the template used by the scanner. The biometric feature constructed in this way most likely is not the same as the one that was used to create the template as information is lost in the process of creating the template. It does resemble the original sufficiently, or has the essential features to fool the algorithm employed by the system, though.

The prevention against fingerprint spoofing has also received attention, for instance from Biosal[122] at the biometric summit[123] 2005 in Miami. This report acknowledges the risks of spoofing and concludes:

> "Compared to other components of the digital infrastructure, biometrics has much higher failure rates. That is, false accept rates are much higher and the ability to spoof biometric systems is relatively easy. If any improvements in overall security system failure rates are to be accomplished, biometrics must be complemented with other forms of physical and logical security"

There are several methods that can be used against fingerprint spoofing[124] :

- supervision of verification, in addition to enrolment
- addition of another token (password, smart card)
- aliveness detection based on recognition of physiological activities as signs of life (see also patent literature [125]
- thermal sensing of the finger temperature
- detection of 3 dimensional shape and pulse

---

[121] http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en

[122] http://people.clarkson.edu/~biosal/research/spoofingfingerprint.html

[123] http://www.wave-report.com/conference_reports/2005/Biometrics2005.htm

[124] http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/Microsoft%20PowerPoint%20-%20SchukersS.ppt%20%5BRead-Only%5D.pdf

[125] http://forensic.to/biometpatent.htm

- pulse oximetry
- ECG
- electrical conductivity of skin

5.2.2.2 Surgery

To change a biometric property without spoofing (for instance, a fingerprint) is only possible with surgery (and only a few cases[126] with transplantation have been reported on this). Concerning iris surgery, there appear to be a few cases where this had an influence on the iris.[127]

Another case that has been reported is the amputation of an index finger of a Malaysian Mercedes car owner.[128] The amputated finger was used to unlock the car's fingerprint access control system. This kind of biometric system could cause a new kind of severe crime of mutilation of the human body.

5.2.3 Conclusion

The preceding examples show that biometric systems are not completely tamper-proof, especially if the equipment is unattended. When investigating evidence from biometric devices, the forensic examiner should therefore consider the possibilities of tampering with the biometric systems, or the possibilities of unauthorized access, before drawing conclusions. A problem with biometric features is that they are not easily revoked or changed if they are compromised. We only have two irises, two hands, 10 fingers etc. A compromised single finger can be replaced by another, but after all ten are used there are no options. There are methods to extract multiple templates from a single biometric feature that allow for template revocation, but these are not employed in actual practice yet (see for instance Linnartz & Tuyl, 2003).

Detecting and addressing fraud involving biometrics is difficult. If the biometric feature is implemented on a smart card to be carried by the victim, and the card, in conjunction with the biometric is used to verify the holder's identity, this practically means that theft of the card, and cloning of the biometric renders the validation useless. The card can only be blocked if the use of the card is validated against a central database which blacklists compromised cards/identities. The card can be revoked, but the biometric remains compromised and can no longer be used without fear of additional ID fraud.

---

126 http://www.scafo.org/library/120604.html

127 http://www.politec.com/asp/BaseTechnologies_IrisRecognition_01.asp#7

128 http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Biometrics at present also represents immature technology, as there are hardly any large scale implementations, let alone independent evaluations of these systems. This is necessary before a wide-scale introduction of these systems is sound.[129]

[129] http://europa.eu.int/idabc/en/document/4066/194

6 Countermeasures

Identity fraud provokes a range of problems that affect individuals, banks, private companies, government agencies, crime investigation services, etc. The central question is how can identity be made more secure? How can data be protected and how can forgery be prevented?

Basically, preventing identity theft is always based on trust that some entity keeps certain information secret, at least in the online world[130], so that only that entity can make use of this secret information. ID fraud may be the result of people not keeping their secrets, but also of machines 'leaking' these secrets. Hence, we have to have:

- Trust in a user, that he keeps certain information (password etc.) secret.
- Trust in the authenticating party to keep the data obtained for and during authentication secret, and not disclose or leak the data to others that may use them for malicious purposes.
- Trust in a device (this means: trust in the producer/verifier of the device), that secret information kept in the device does not under any circumstances leave the device (tamper resistant hardware).
- Trust in protocols and software implementing these protocols (this means: trust in the producer/verifier of the software and protocol), that certain assumptions about resistance against attackers are true.

ID-related crimes involve people (victims and culprits) and machines, and countermeasures can address both people (social aspects, the first bullet) as well as the machines and the interaction between the two (technical measures, the latter two bullets). Often, all three types of trust are needed in order to prevent identity theft as much as possible.

Current initiatives

In the fight against identity fraud, there are a number of initiatives from national governments (in particular law enforcement agencies) and European-wide initiatives. A prevention expert group representing all concerned parties, such as national authorities, banks, law enforcement agencies, consumer associations, is established (Tiné, 2004). Its main objectives are to discuss new fraud prevention issues and identify preventative measures. Law enforcement initiatives focus on the diffusion of information and training by means of forums, workshops, dissemination of guidelines, and other methods.

From a commercial perspective, Visa and MasterCard have recommended the implementation of an architecture/set of protocols named 3D Secure. This protocol redirects financial

[130] In the offline world an important mechanism for providing trust is recognizing known people.

transactions to the banks. The verification of the identity of the buyer is performed by the bank instead of the seller. This would transfer the responsibility from the seller to the bank and banks are therefore reluctant to accept this. Instead some banks have installed other systems of identification, e.g. ID-tronic[131] in France.

Generally prevention programmes (Sood 2004) or associations (e.g., CIFAS) against identity theft and identity fraud aim at establishing a privacy task force and providing some recommendations concerning identity recovery plan.

6.1 Social and technical guidelines on preventing ID-related crimes

6.1.1 Socio-economic guidelines

The socio-economic analysis in chapter 4 provides us with a starting point to elaborate on socio-economic measures that can be taken to address ID fraud.

1. Raise awareness for the social and economic consequences of ID fraud:
   a. Society pays for convenient, but weak authentication combined with strong authorisation with the loss of money and trust.
   b. But society equally pays for security with operational costs and loss of convenience, liberty, liberality and freedom.
2. To balance authentication and authorisation (see chapter 4.7.1) feed-back control systems should be used. These systems need a certain time for the balancing process which should be granted to them. To push new technologies for authentication into the market while security and privacy aspects are not discussed and properly resolved will only increase people's distrust in online transactions, leading to calls for more security measures (cycle of distrust).
3. The cycle of distrust above must be slowed down. This could be achieved e.g. by
   a. Using authentication schemes proportional to the communicational context and purpose; the authentication should only entail the information required for the steps to be taken within the authentication / authorisation. Especially personal identifiers granting strong rights (e.g. the credit card number) should not be used where simply a proof of the age or the determination of the social system and the role taken therein is needed. This means creating and using a set of

[131] ID-TRONIC is a means of electronic payment promoted by the "caisse d'épargne". It allows Internet payments without having to communicate a credit card number. Before any transaction, the buyer, and client of the bank, has to fill an online form on the bank site with his banking co-ordinates. He then receives an ID-TRONIC number. When he makes a purchase, it is this number which he must use with another string of figures which is sent him by SMS for each purchase. This system guarantees confidentiality and minimizes the risks of fraud.

verifiable credentials, such as a (biometric) smart card that can only be obtained at a certain age.

b. Using, in addition, socially accepted technical methods for authentication. In the context of the communication from organisations to their clients, which takes place only once a month, a complicated and often to be changed password usually will not lead to improved security (as it probably would in the context of the day to day communication within an organisation) as clients will document the complex password somewhere, usually under the keyboard. Obviously, this doesn't really improve security.

c. Improve the security of authentication processes in accordance with cause-effect-correlations. Including biometrics in the passports to fight ID fraud and to fight terrorism (like the 9/11-attack in the USA), for instance, is a bad example in this respect: all terrorists had valid passports, so biometrics in the passport will not prevent terrorist passing the border. The problem was not the passport itself, but the process of issuing them and the process of granting visa. The argument that we need an improved passport doesn't meet the cause for the problem in this case.

d. Using multiple independent and technically strong authentication system if higher security in authentication and authorisation. In addition the authorisation provided by each of them should be limited (decoupling of systems with high security demands). Single Sign On may be convenient, but it also lowers security in the end as it makes the corresponding identifiers more attractive for identity thieves (Kent and Millett 2001).

6.1.2 Technological guidelines

Social measures can only go some way in improving online security and fight ID fraud. Awareness can be raised, people can be taught to behave more responsible with respect to their ID data, but in the end culprits find and exploit technical leaks in systems. Therefore, also technical measures have to be taken.

Current national actions in Europe and some European actions, e.g. the European passport, focus on the establishment of a digital identity document to deter identity fraud by combining the use of biometrics and smart cards. These technologies are discussed further below. Particular attention is paid to the use of privacy-enhancing technologies (PET). The objective is to demonstrate how the problem of identity theft can be tackled without necessarily surrendering privacy in the process.

On the basis established methods for a risk assessment such as described in the IT Baseline Protection Manual[132], we can list a number of guidelines for authentication systems. The following guidelines a are derived from the socio-economic chapter and the technical paper that was prepared for the FIDIS wp5/wp8 workshop in May 2005. The guidelines can be presented on two levels:

1. Authentication technologies in general
2. More secure authentication

6.1.2.1 Authentication in general

The authentication should be kept as general as possible, no unnecessary data for the purpose of authentication should be required and used (data minimisation). A positive example in the offline world is the anonymous purchase of goods paid in cash in a shop; no personal identification is required. A negative example is the use of a credit card number to verify that a customer is older than 18 years. To meet higher security needs generally more personal data are required.

Generally, active authentication should be used. Following the principle of informational self-determination, which is coherent with the EU Data Protection Directive and which can also be derived from Fair Information Practices, the user should be in control *where, when* and *for what purpose* she is authenticating. Especially passive or behavioural biometrics should only be used within active authentication procedures.

Technical authentications should be socio-psychologically accepted. In many cases authentication systems are implemented that are not accepted in a given communicational context and are therefore bypassed. One example is the use of a complicated password for authentication that is rarely used (e.g. once per month). Most users will store the password in a non secure way (e.g. under the keyboard)as they are unable to memorise these passwords. The aim of improving the security by using a strong password cannot be reached. In another context e.g. where used every day in an enterprise by employees a strong password may be a good and accepted solution.

Do not use irrevocable authentication data (e.g. a key or token). If these get stolen, abuse cannot be stopped easily. Many kinds of biometrics, such as the face when automatically recognised are difficult to revoke – one cannot change his face easily. Cryptographic keys in contrast are comparatively easy to revoke and to exchange against new keys. Of course the revocation process has to be defined and prepared in advance: It should be clear under which conditions authentication data is to be revoked and how this is to be performed (e.g. authenticated revocation).

---

[132] Download: http://www.bsi.de/english/gshb/manual/download/

Use methods for authentication without internal verification. User name, key and additional information / secrets (like the date of birth) should not be aligned by an algorithm. Once the algorithm is known (or reasoned from known data combinations), missing parts of this combination can be calculated or virtual identities can be created.

Do not use authentication systems that are difficult to update. Generally security requirements are rising and the enrolment of a new authentication system can be expensive, especially when used by numerous clients.

6.1.2.2 More secure Authentication

For higher security needs use two or more factor authentication. Use a combination of knowledge, possession and something you are which all have to match the authentication challenge to improve security.

To further improve security the different factors should be verified using independent authentication systems.

Do not use centralised authentication systems for multiple purposes when higher security is needed. Authentication systems should be bound to a specified purpose. The use of context-specific keys is a method to raise the hurdles for identity thieves. Single Sign On (SSO) in contrast is convenient, but less secure.

Use one-time authentications where possible. One-time authentications cannot be reused and are therefore less vulnerable to identity crimes as repeat identifiers.

Use two-way authentication to improve security where needed. Usually organisations authenticate clients in a one-way process, while the client can't authenticate the organisation sufficiently (see chapter 5.1.3). In addition to the one-way authentication, the client authenticates the organisation e.g., by using certified signatures for the exchange of messages. Two-way authentication can make certain attacks like phishing or man-in-the-middle-attacks much more difficult and thus improves security.

6.1.3 Digital identities

Generally, *partial digital identities* identified by *digital pseudonyms* are *the* means to model identity within the digital world. This section describes a number of relevant terms related to digital identities from the perspective of preventing identity fraud based on Pfitzmann and Hansen (2006).

Digital identity denotes attribution of properties to a person, which are immediately operationally accessible by technical means. A digital identity is always a *partial identity* (Pfitzmann and Hansen 2006).

Partial identities are subsets of attributes of a complete identity in the real world. On a technical level, these attributes are data. Thus, a *pseudonym* might be an identifier for a partial

identity. Whereas we assume that an identity in the real world uniquely characterizes an individual (without limitation to particular identifiably sets), a partial identity may not. This enables different degrees of anonymity. However, for each partial identity appropriately small identifiably sets may be found, such that the partial identity uniquely characterizes an individual.

The identifier of a digital partial identity can be a simple e-mail address in a newsgroup or a mailing list. Its owner will attain certain reputation. Digital identity should denote all those personally related data that can be stored and automatically interlinked by a computer-based application.

With regards to preventing identity theft (i.e. regarding accountability), a digital pseudonym needs to have special properties:

- It must be unique as ID (at least with very high probability) and
- must be suitable to be used to authenticate the holder.

A *digital pseudonym* having such properties could be realized as a public key to test digital signatures where the holder of the pseudonym can prove holdership by forming a digital signature which is created using the corresponding private key (Chaum 1981). The most prominent example for digital pseudonyms are public keys generated by the user himself/herself, e.g., using PGP.

A *public key certificate* bears a digital signature of a so-called *certification authority* and provides some assurance to the binding of a public key to another pseudonym, usually held by the same subject. In case that a pseudonym is the civil identity (the real name) of a subject, such a certificate is called an *identity certificate*. An *attribute certificate* is a digital certificate which contains further information (*attributes*) and clearly refers to a specific public key certificate. Independent of certificates, attributes may be used as identifiers of sets of subjects as well. Normally, attributes refer to sets of subjects, not to one specific subject.

For preventing identity theft, also the following properties of pseudonyms may be of importance:

- limitation to a fixed number of pseudonyms per subject (Chaum 1981; Chaum 1985; Chaum 1990);
- guaranteed uniqueness (Chaum 1981; Stubblebine and Syverson, 2000);
- (controlled) transferability to other subjects,
- convertibility, i.e., transferability of attributes of one pseudonym to another (Chaum, 1985, Chaum, 1990);
- possibility and frequency of pseudonym changeover;

- validity (e.g., guaranteed durability and/or expiry date, restriction to a specific application);
- possibility of revocation or blocking.

Limitation to a fixed number together with guaranteed uniqueness is necessary in cases where a person needs to be non-ambiguously recognizable by her pseudonym. Controlled transferability to other subjects is important for scenarios where delegation of rights is needed. For instance in case where there are organisational rules for substitutes, a pseudonym can be transferred to a substitute for some defined time frame. Convertability, as well as the possibility of pseudonym changeover is a basic building block of privacy enhancing identity management (see section 6.2.2 for more details). Validity verification and possibility of revocation or blocking are essential features for preventing from identity theft in cases, where a (business) relation ends or gets compromised (e.g. by a compromised a secret key for communication). In such cases it is important to be able to declare a used pseudonym invalid in order to prevent from fraudulent usage of this pseudonym by others.

In addition, there may be some properties for specific applications (e.g., addressable pseudonyms serve as a communication address) or due to the participation of third parties (e.g., in order to circulate the pseudonyms, to reveal civil identities in case of abuse, or to cover claims).

Some of the properties can easily be realized by extending a digital pseudonym by attributes of some kind, e.g., a communication address, and specifying the appropriate semantics. The binding of attributes to a pseudonym can be documented in an attribute certificate produced either by the holder himself/herself or by a certification authority.

The concept introduced and the properties associated with them can be used to assess some of the technologies that can be used to limit the risks of ID-related crimes.

The guidelines discussed here are not intended as a checklist that has to be completed in order to build applications that are safe from ID fraud. Implementing all of them would probably even result in a system that is not usable at all. A balance between usability and security will have to be made. The guidelines presented can serve as a starting point for finding the proper balance.

6.2 Authentication technologies

In the following sub sections we discuss three general technologies that affect authentication in different ways:

- Biometrics
- Identity management
- Trusted platform module

6.2.1 Biometrics

All biometric authentication systems involve two steps: (a) an enrolment process and (b) a matching process. The first step is the most critical as it involves the binding of the individual to a digital identity. Initially, the person provides evidence of their identity and after the verification of the provided identity against an existing ID document, such as a passport for instance, they present the required biometric information by using a device (camera, scanner, etc). The specific distinctive features presented to the biometric scanner is next parameterized by a function or converted into a mathematical template. The template may be, or should be, encrypted and stored in a database linked to the individual's identity and/or a smart card (the last one provides a combination of the mentioned methods) and constitutes the reference data to which the respective biometrics data captured during the "matching" phase are compared.

The enrolment process is substantial for the operation of a biometrics authentication system, and thus preventing identity theft during this process is critical. An identity thief, who may have obtained the necessary identification means for enrolment (for instance a passport), and who, if necessary, has forged some information on this ID (such as replaced the victim's photograph with one matching the culprit), may enrol his or her own biometrics with the stolen identity before the victim becomes aware of the thief's activity. This enables the identity thief to claim the victim's identity.

ID fraud may be detected during this process due to the uniqueness of many human characteristics. For instance, if the fraudster has already created a true or false identity and attempts to establish a second one through the same enrolment system, using the same biometric information (*i.e.*, face image, fingerprint, iris scan, etc.), the system may detect that the biometric data presented already have been registered and thus notify about this activity.

After enrolment, authentication on the basis of the enrolled biometrics involves the user to provide her biometrics. These will be compared against the reference data stored into the repository. During this process the level of matching is determined taking into account the type of biometric and a threshold for the type of biometric used and the demands of the specific application. These parameters control the False Acceptance Rate (FAR), falsely accepting a biometric as belonging to the person who presents them, and the False Rejection Rate (FRR), falsely rejecting a person as being as being the proper holder of the biometric characteristics. Usually these are controllable parameters, although each technology has its baseline accuracy. An application requiring a high level of security during authentication would require a high threshold value, usually leading to a high FRR, too many people are rejected, whereas an application which includes low risk would be more flexible and would thus settle for a low matching score. The latter usually means a higher FAR; too many people are accepted, including possible imposters.

As already mentioned in section 5.2.2.1, biometrics spoofing is a threat biometrics authentication systems should deal with. Especially since biometrics are not generally secret

(voice is recorded, facial images can be easily captured, fingerprints are left at any place the persons touches) and there is the limitation of not having the opportunity to change one's biometrics just like a password and the options are not many (two eyes, ten fingers). Hence anti-spoofing measures need to be implemented.

The performance of a biometrics authentication system – and thus its security - is affected by the accuracy of the technology itself, which varies from very accurate (DNA for instance), to fairly accurate (iris, fingerprints)[133], and the quality of the enrolled biometric features. Enrolments of poor image quality or few biometric features probably raise the need of setting thresholds to rather insecure levels - so that the system performs "acceptably" for the registered persons – increasing its vulnerability in spoof attacks. Hence, enrolments of good quality lead to the optimization of all aspects of performance of a biometrics system. Supervised enrolment by trusted and suitably trained staff can further improve the quality and reliability of the enrolment data.

Systems designers that show no great interest in security (authentication techniques used in the context of entertainment systems for instance), and hence do not invest sufficient amount of money in this area, could reduce the possibility of biometrics spoofing by requiring the provision of multiple biometrics data to the system (for instance the use of 2 or 3 cameras acquiring simultaneously facial images of the person to be authenticated - both frontal and side views), or the combination of biometrics with another means of authentication (smart card, PIN, etc.).

In cases of need for a high level of security, a supervised - by trained and trusted staff - system is likely to be much harder to spoof and also the risk of being presented false biometric features by the person to be authenticated is smaller. Nevertheless, significant research efforts are invested to make biometrics authentication systems smart in distinguishing between real and fake data provided to them. One example of the promising results of this kind of research is the implementation of checks based on distinguishing real faces from photographed faces by looking for typical reflection patterns of photographic paper in the camera image used for authentication.

Aiming at preventing spoof attacks with the provision of biometrics from artificial equipment or even cadavers, companies and researchers develop techniques that perform "live-ness checks" - technological countermeasures to spoofing – that must be applied at the same time and place that the biometric features are captured. During these checks one or more checks on responses and measurements take place, such as the presence of pulse, thermal measurement, electrical measurement, etc. Recently, for cameras "live-ness detection" has been developed[134] that makes use of intrinsic facial movements that the camera can "see", capture and analyze,

---

[133] See IPTS 2005 for an overview of relevant parameters for the various techniques.

[134] More info can be found on http://www.zdnetasia.com/news/security/0,39044215,39283698,00.htm

and thus get clues that this is live skin and a live human being (looking for natural facial movements such as the closing and opening of eyelids).

Another anti-spoofing technique is based on an interactive biometrics authentication system with the use of challenge/response. This technique is most often met in voice recognition biometrics systems. The system asks the person to speak a number of words/numbers in random order, so that both the voice features and the order of repetition of the words/numbers can be checked.[135]

Generally, biometric authentication systems strive to make computer systems and networks more secure, by eliminating the risks that follow the use smart cards, PINs and other normal authentication methods. And, as James Childers states: "Security is more than just creating and implementing an impenetrable system... It is a mind-set that every system is penetrable, all solutions are fallible and the only secure system is one that is diligent in its methods, rooted in the fundamentals of secure credential management and uses multiple methods of authentication."[136]

6.2.1.1 Behavioural biometrics in prevention of ID fraud

Also behavioural characteristics can be used to prevent ID fraud. For instance, keystroke dynamics can be used for authentication purposes, as every user has unique typing characteristics on computer keyboards: the keystroke latencies – including the time intervals between keystrokes, hold times, typing error frequency and force keystrokes – form a digital signature of the user. This technology is based on the detection of an individual's typing patterns on a keyboard and their comparison against patterns previously enrolled.

The main application of this biometric is in protecting passwords; in other words, in providing greater assurance that a password was actually typed by the person who enrolled it. As passwords can be guessed or stolen, their protection can be enhanced by this relatively simple: timing information concerning the user's typing of their password as well as the password itself is logged by the system, and thus a newly entered password is classified by a pattern recognition system as matching or differing from the logged timing patterns. In this way any application able to reliably measure the timing of a user's typing can also try to perform identification or verification of the user. This behavioural biometric can provide protection against external and internal attackers. Protection against internal attackers (within a given system) can be achieved through the encryption of the passwords stored in the database with the person's biometrics – in this case the keystroke dynamics measurements during the password typing of the person owning the password. In online settings (external) the measurement of the typing characteristics has to be done on the client

---

[135] Anti-spoofing techniques for Voice, Judith Markowitz, Biometric Consortium Conference BC 2005

[136] http://www.biometricsdirect.com/Content/Gummy_Fingers.htm

side. This possibly introduces inaccuracies due to dependency on the user's hardware in an uncontrolled environment and hence introduces its own type of vulnerability: spoofing typing behaviour.

6.2.1.2 Physiological biometrics in prevention of ID theft

Facial recognition is among the primary human perceptual capabilities. An authentication system based on computerized facial recognition offers advantages, such as low cost, unobtrusiveness, easy access (the face is something you are never without!). The commonly accepted approaches use the eigenfaces or geometric transformations to perform the human identification task. However, the main drawback of these techniques is their demand in computational resources, which can be a limiting factor for real-time applications.

Face recognition systems attempt to perform measurements of some nodal points on the face (the distance between the eyes, the distance from eye to mouth, the width of the nose, etc) or use appearance-based classifiers. The presence of occluded faces/bodies, complex background and foreground, moving background, complex human movement, varying lighting conditions or strong resemblance between two people (e.g. twins) are factors that make the human detection, localization and identification processes a difficult, and thus challenging task. The enrichment of the human identification process with human body modelling information and the use of a stereoscopic camera system can lead to the improvement of the performance of these processes in complicated situations. A major advantage of face recognition technology is that the hardware required (a camera) is relatively simple compared to other kinds of biometric devices, and thus it may be added to any existing surveillance or multimedia system.

The reinforcement of security in mobile devices through face authentication of the owner of the device is an example of application of this biometric in preventing identity theft. Given the fact that the functionality of mobile devices has been enriched with a variety of new services, including personal data, such as address book, payment data, and schedules, increase the value of these devices for culprits, and hence the threats of identity theft increase. The protection of the information held by these devices has become essential. Camera equipped mobile devices can be supplemented with facial recognition software to increase their security.[137]

Biometrics as explained in the preceding chapter, itself has vulnerabilities, and hence are not sufficient in their own right. Biometric technology can best be used in combination with other biometrics or with traditional security methods (passwords, identity cards, smart cards, etc). A

[137] Similar approaches of securing mobile phones are the experiments Philips is conducting with measuring ear canal geometry by means of an extra microphone in cell phones.

smart card can be used to store all types of data; however it is mainly used to store encrypted data, human resources data, medical data, financial data, and biometric data.

6.2.2 Identity management

A second way of limiting the risks of ID-related crimes, is identity management. Both in online- and offline transactions, users are asked, and tend to reveal significantly more information than necessary for the transaction. If a user is requested to prove she is over 18 years of age (for example to get access to a bar), she normally has to present her identity card, which reveals her exact birthday, full name, address, and various other data that are of no relevance to the patron of the bar. Worse, Internet sites that demand a proof of the user's age tend to obtain this by demanding a credit card number (assuming that only 18 year olds have credit cards). It is obvious that such a situation is paradise for identity thieves, who can obtain volumes of information about a user by simply claiming to check her age.

One of the main means in protecting a user's identity from being stolen is to be as restrictive as possible with revealing identity related information. In each transaction, the transaction partner has to be provided with exactly the information needed to complete the transaction, and nothing more. Techniques to accomplish this are already under development in the privacy area, and allow users to manage their identities in various ways. The EU funded FP6 programme PRIME is an example of such an approach.[138]

Identity management systems typically provide one or more of the following capabilities.

A *pseudonym system* allows a user to use different, unlinkable identities for different transactions. A simple, homemade way is, for example, the use of different email addresses for different purposes

There are a number of open issues involved to maintain the unlinkability of the pseudonyms, especially at the interface between the Internet and the real world. For example, a user may still want to be able to pay for a service. Although some credit card companies work on one-time credit card numbers, this usually still requires a unique link to the user.

Also, there are attacks possible on the lower protocol and network layers; while different email addresses can help against an attacker that tries to obtain information about a user by means of search engines, users still tend to access all their accounts from the same computer. Unless anonymous network access is provided, a sufficiently sophisticated attacker can abuse this to determine the link between the pseudonyms. Even the fact that many private users make use of randomly assigned IPs (by ISPs), this no longer guarantees unlinkability given the fact that even low level TCP/IP messages contain unique fingerprints due to machine specific delays (Kohno et al 2005).

---

[138] See http://www.prime.org for more information.

Finally, the main task a good pseudonym system has to do is to help a user to manage all her pseudonyms – if users take their anonymity seriously, they will have more pseudonyms than transaction partners, which is more than one can expect a person to handle. A nice example for such a system is the cookie cooker, a local web proxy that generates and manages passwords, removes traces (such as cookies), and even fills out web-forms with plausible fantasy data.

A Credential System (e.g. Camenisch and Lysvanskaya 2001) assists a pseudonym system if the user is supposed to prove that she satisfies some properties. Suppose again that a website requires a user to prove she is over 18 years of age. If pseudonyms are used, the user would need some trusted entity to certify that this pseudonym belongs to a person age 18 or higher, and she has to be prevented from "lending" her pseudonym to a third party. With a credential system, a user can get credentials on certain properties, and later prove possession of those credentials without revealing any user related information. This property allows the user to prove properties independent of the pseudonym she currently uses; all certification has to be done only once. Instead of showing the credential (i.e., a signature from the credential issuer) itself, the user can prove that she knows this signature. Using new zero knowledge techniques, this can be done in a way that the verifier at the end is convinced she knows the signature, without having any more information about it. Especially, if the same user is to show the same credential again, the verifier will not be able to link the two credentials to the same person.

6.2.3 Trusted Platform Module

While a number of techniques exist that allow a user to authenticate herself, most of these techniques come with a number of problems. Unless an authentication device is used that has some computing power on its own, a user transmits all information needed for the authentication every time the authentication process is required. This allows a rogue to obtain this information not once, but every time authentication takes place. This makes often used identifiers, such as credit card numbers and the American social security number particularly vulnerable for misappropriation, and hence if someone presents these data it actually does not authenticate at all as virtually anyone may have obtained the data. Furthermore, some authentication information carries sensitive information; an iris scan, for example, may reveal information on the user's health status. Even if smartcards are used, the problem is not solved; as smartcards can easily be lost or stolen, secondary authentication is needed if this technology is used.

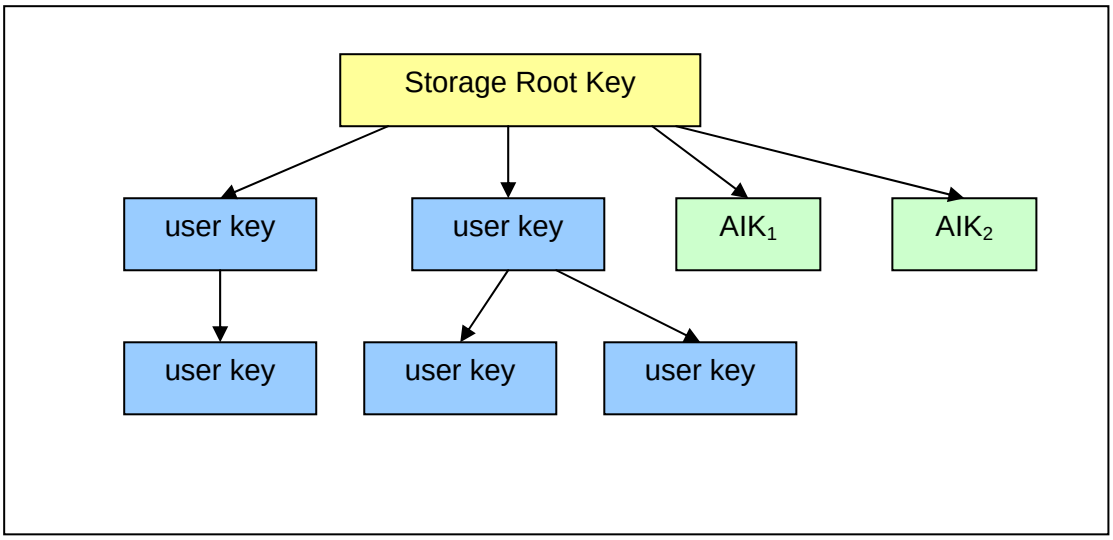


Figure 14. Keys managed by the TPM.

Trusted Computing is a relatively new concept that can assist current authentication methods by securing the infrastructure used for authentication. The essential goal of this technology is to create trust in computing platforms (which may be Personal Computers, but also smartcard readers). To this end, a consortium of about 100 major IT companies has defined a standard for an small, cheap, and more or less tamper resistant security module (Trusted Platform Module, TPM). This module can protect keys, execute some cryptographic functions, and – most importantly – can attest some information about the platform to outside parties.

6.2.3.1 Secure key storage

A TPM can – comparable to a smartcard – securely store users' keys. As a TPM is platform rather than user bound, and may be utilized by various applications, the number of keys it has to maintain can be rather high. As the chip has to be as cheap as possible, while permanent storage of keys on such a chip is rather expensive, this presents designers with contradictory requirements. To solve this problem, the TPM does not store all keys in its internal memory. Rather, it stores one *master key* (the *Storage Root Key, SRK*), which is generated once the chip is initialized (*owned)* by the user. It then allows creating additional keys, which are encrypted with the SRK, but stored externally by the operating system. It is also possible to encrypt keys using such second level keys, i.e., the keys are encrypted in a tree-like structure. This allows, for example, giving every user on a platform his individual master key, which is then used to encrypt the different application keys required by this user.

Each key is stored alongside with a number of properties that define its usage. Most prominently, a key can be marked as *migratable or non-migratable.* The later keys are bound to the platform, and cannot be copied anywhere else; it is impossible to steal such a key (even with the users consent) without stealing the entire computing platform.

6.2.3.2 Self- and remote authentication

One of the core ideas in the trusted computing concept is that the TPM offers trustworthy information on what is going on a user's machine. Currently, every attacker that gains access to a machine can make himself at home there – tools exist for both Windows and Linux to create backdoors that are practically undetectable. Thus, even if the keys are protected and cannot be removed from the platform, the attacker can freely use them at any time (provided he stole the authentication information as well).

In the TCG (Trusted Computing Group) concept, the BIOS (and ideally, the operating system as well) report checksums of the start-up sequence to the TPM, which stores them in a secure way. By the time a malicious application gains control, its existence has already influenced the checksums stored in the TPM, which allows detection of the imposting code. To utilize the checksums, the TPM can now sign and output them (which can be used to convince an external party that the platform has not been compromised). Also, it is possible to seal keys with these checksums; if the platform does not boot into the state defined at key generation, the TPM will refuse to use the corresponding key.

6.2.3.3 ID-Management

As mentioned previously, one of the prime weapons against identity theft is the use of pseudonym systems – if a user can prove attributes (e.g., being over 18 years of age) without revealing any other information relating to her identity (e.g., her address or credit card number), it becomes much harder to carry out identity theft. The TPM can be used to provide for the proper credentials to facilitate this scheme.

For privacy reasons (and as a result of the bad experience with Intel's processor serial numbers) the TPM has two build in mechanisms to support pseudonyms.

The first mechanism is rather straightforward and uses a trusted third party (TTP). The TPM sends its certificates, a pseudonym, the public EK and auxiliary data to the TTP. The TTP then verifies the data and issues a certificate for the pseudonym. This certificate is then encrypted using the public part of the endorsement key, so that only the TPM can decrypt it. The result is a pseudonym that is not linkable to the identity of the TPM by anyone but the TTP, but cannot be used by anyone but the TPM.

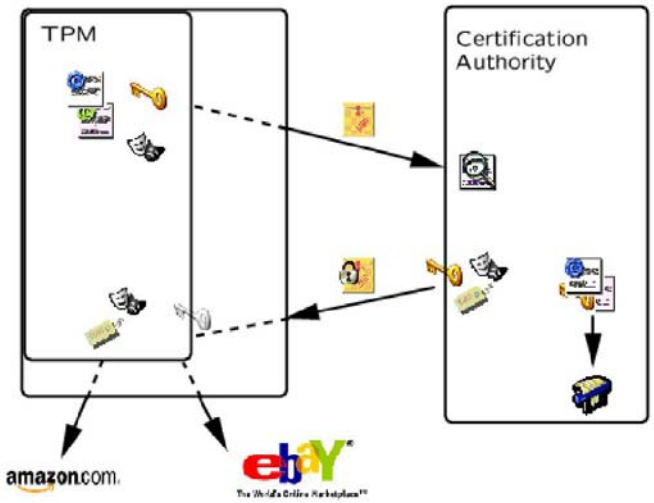


Figure 15. Use of pseudonyms certified by a Trusted Third Party and encrypted using the TPM

As a second mechanism, especially to handle pseudonyms in situations where no trusted third party is available, the latest version of the TPM specification also defines a zero-knowledge based protocol to maintain pseudonyms, the *Direct Anonymous Attestation* protocol. This protocol allows the TPM to prove that it is a real TPM without revealing its identity to any party at all. In principle, it is thus possible to obtain certificates and create pseudonyms without revealing ones real identity even to the issuer. Unfortunately, as the protocol is not designed to demonstrate anything but the origin of the TPM, the actual implementation of such a scheme still requires some research.

6.2.3.4 Shortcomings

Key migration

If a key is marked as *non-migratable* – which may well be the case for critical identity related keys - some problems occur if the key actually needs to be migrated, for example because the platform broke and needs to be repaired. The TPM Specification does suggest a mechanism to move such a key to another TPM, but it is only optional, rather complex (it requires active involvement of the platform manufacturer) and is thus nut implemented for any existing TPM. The main problem here is that one TPM cannot recognize another one – it thus has no way to ensure itself that the key is moved to another TPM (which then offers the same protection) or to the outside world.

A related problem is a user who uses multiple platforms, for example a home PC, a laptop and a cell phone. As the keys are bound to a platform rather than a user, some auxiliary mechanisms may be needed for roaming users.

Key revocation

As mentioned above, the TPM does not store most of its keys itself, but delegates this task to the operating system. While this helps to keep the costs down and allows for a practically unlimited number of keys, it also takes away some control over the keys – mainly, the TPM is not capable of reliably deleting keys unless it deletes the Storage Root Key (and thus renders all keys maintained by that TPM useless). For individual keys, however, anyone who has a copy of the encrypted key, the necessary authorization information and access to the TPM (which is well plausible for a machine with several users) can use this key.

Secure operating systems

While Trusted Computing can be used to solve a lot of issues around device security, it is still insufficient as long as the higher level operating system is insecure. The whole design only makes sense if used as the lowest security layers, with further secure systems building on top of it. The next step towards real security is to build a Trusted Computing enabled microkernel operating system (as done, for example, in the European Multilateral Computing Base). Those systems can provide users with a trusted viewer (so they know, they authenticate to the system, they think, they authenticate to, unlock their smartcard, they think etc), which can not be interfered with by other applications running on the same machine.

6.3 Conclusion

This chapter has discussed some of the social and technical measures that can be taken to limit the risks of identity fraud. It shows that social measures have a limited usefulness if technical measures are not taken. Users and service providers need to become aware of the risks of life online and also the burden of taking measures has to placed on the actors that can actually make a difference and perverse incentives and other externalities have to be addressed. Yet, this only makes sense if proper technical measures are also taken otherwise the backdoors will not be addressed.

The technical measures increasingly gain attention of academics and industry. The brief exposition in this chapter shows some promises, but also many problems that remain to be solved. For the short term we may therefore, unfortunately, expect many cases of ID-related crime.

7 Conclusions and further work

In this document we have discussed ID-related crimes from different perspectives. (For a summary of these perspectives, see the Executive Summary.) Much work remains to be done in order to gain a better understanding of the rapidly evolving phenomenon of ID-related crimes. The chapters brought together in this document have been written by different researchers, from different backgrounds and disciplines. When read in combination, the chapters suggest at least two things: first, that there is no consensus on the exact phenomenon we are talking about and just what constitutes ID-related crimes, and second, that legal, social-economic, and technical aspects interact, showing the need for a combined approach towards combating ID-related crime. As the conclusion of this document, therefore, we suggest that at least the two steps need to be undertaken: searching for a common ground in terminology, conceptual framework, and definitions, and setting an agenda for joint research.

7.1 Towards talking about the same thing

7.1.1 Terminology

In this document, many terms have been used to describe a single or, more likely, multiple phenomenon: ID theft, ID fraud, ID crimes, ID-related crime, ID mix-up, ID change. The scheme of Figure 4 in Chapter four gives a first indication of how all these terms might relate. We (editors) think such a scheme could be extended and filled in further, in order to clarify the various forms of ID 'something' that we are talking about. For example, we could extend Chapter four's figure 4 as follows:

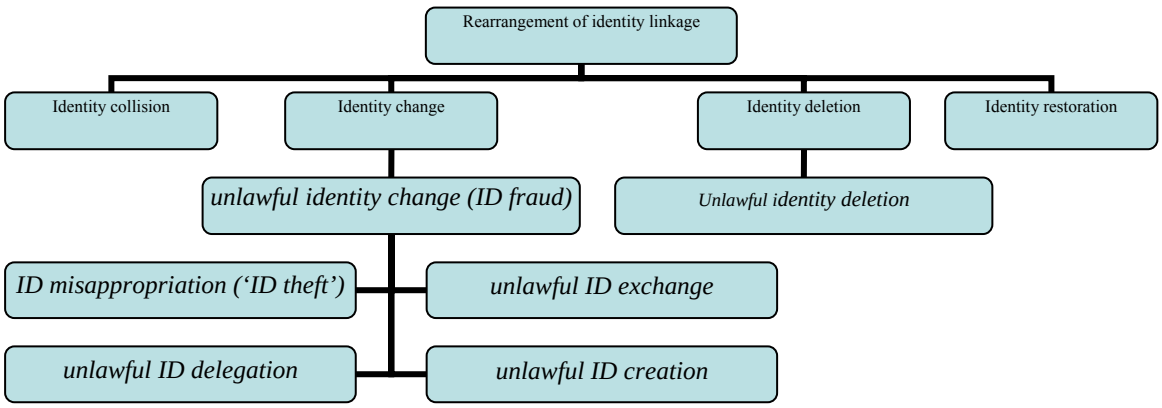


Figure 16. Sample taxonomy

The upper layers indicate types of ID-related activities, both lawful and unlawful. The lower, italicised, blocks indicate the subset of unlawful ID-related activities, which we might group

together under the term ID-related crime. Although there is not yet a consensus of which term we should use, it seems that a common interest can be found in researching the various acts in the italicised blocks (even if some researchers focus only on a subset of these), and the term most often used for this is 'ID-related crime'. Further research and discussion is needed, however, in order to create a taxonomy and related terminology that can be used as the basis for interdisciplinary research.

7.1.2 Conceptual framework

Related to the terminology issue is the conceptual framework. Most of the research in this document focuses on ID fraud, notably ID misappropriation ('ID theft') or unlawful ID creation. This activity can be studied – as indeed it should presumably be combated – from a combination of legal, social-economic, and technical perspectives. The chapters as well as the discussion of the May 2005 workshop indicate, however, that there is no consensus yet on just which activities fall within the term of ID fraud or exactly which activities are found relevant to be studied. In fact, several structures of ID fraud have been suggested in the literature and at the workshop:

<table>
<tr><th>4 steps (Mitchison et al.; TILT)</th><th>2 steps (ICPP)</th><th>4 steps (Karlstad)</th><th>2 steps (VIP)</th><th>common ground</th></tr>
<tr><td>fishing</td><td rowspan="2">assuming an ID</td><td>collection</td><td rowspan="2">profiling</td><td rowspan="2">1. creating an ID</td></tr>
<tr><td>misappropriation</td><td>aggregation
ID creation</td></tr>
<tr><td>misuse</td><td rowspan="2">ID fraud</td><td rowspan="2">criminal act</td><td rowspan="2">malicious intent</td><td rowspan="2">2. unlawfully using an ID</td></tr>
<tr><td>criminal act</td></tr>
</table>

Table 9. Decomposing ID-related crime.

As can be seen from this table, there is agreement on the two major steps: 1) *creating* an ID, and 2) *using* this ID. Both steps can be subdivided in various ways, however, depending on the point of view. From a legal perspective, for example, one could distinguish in the 'use' stage the preparation of abuse (such as possession with the intent to use a false ID) or an attempted crime from the actual abuse or completed crime. From an economic perspective, this also makes a large difference, since the first does not result in actual damage, whereas the second (usually) does. From a technical perspective, however, the distinction need not be relevant: once the false biometric passport has been created, it is technically immaterial whether it is used or not.

Another issue for further research is therefore to develop a shared conceptual framework consisting of the various steps that need to be distinguished in ID-related crime from the various disciplinary perspectives.

7.1.3 Definitions

From the preliminary discussion of definitions in Chapter 2, a working definition was extracted:

> ID fraud is when someone with malicious intent consciously creates the semblance of an identity that does not belong to him, using the identity of someone else or of a non-existing person.

(We leave aside here the need for a more general definition, since ID fraud is only a subset of ID-related crime, as we discussed above. Definitions are needed of both 'ID-related crime' and 'ID fraud'. Here, we focus on the latter, since this subset is at the core of most of the discussions in this document.)

Even if this definition of ID fraud appears better than several other ones, various elements of this definition are contentious, as emerges from the chapters in this document and from the discussion at the workshop. To mention a few:

- *intent*: in terms of damage, unintentional ID fraud can be as devastating as international ID fraud, and from a legal perspective, unintentional – but grossly negligent – acts are also sometimes criminalized; should malicious intent be part of the definition?
- *consent*: one can distinguish situations where the ID of someone else is appropriated without knowledge and consent of the person from situations where there is consent. However, the former does not necessarily constitute fraud (although it usually will), e.g., when a girl uses her mother's bank card to buy candy; and consent does not always mean that no crime is taking place, e.g., when two brothers exchange clothes in prison so that the convict leaves the prison while his innocent brother remains in the cell. Moreover, from a legal perspective, the presence or absence of explicit or implicit consent may be relevant when discussing civil liability. Should consent somehow be part of the definition?
- *use*: the definition given only comprises acts where the false ID is actually used; as noted above, ID fraud comprises also the preparatory step of creating an ID, and so, this should probably somehow be included in the definition; from a legal perspective, it should be discussed whether only the unlawful use of an ID should be criminalized, or also the preparatory step(s);
- *harm*: the definition does not mention actual harm, but of course it makes a difference whether or not ID fraud results in actual damage – material and/or immaterial; related

to the previous bullet: should the mere risk of damage be criminalized or otherwise countered, or should we focus only on harmful acts as such?

To show where such elements lead, one can adapt the working definition in various ways; to name two, rather extreme, examples:

1. ID fraud is when someone creates the semblance of an identity that does not belong to him (of someone else or of a non-existing person) with the intent that it be used for a legally relevant act. [broad version]
2. ID fraud is when someone with malicious intent creates the semblance of an identity that does not belong to him (of someone else or of a non-existing person) and causes damage by using this identity for an unlawful purpose. [narrow version]

When discussing the precise formulation of a definition, it should also be questioned whether a single definition ought to be developed, or whether different definitions should be drafted for use in different contexts. A legal definition need not necessarily be the same as a technical definition (and it would presumably be hard to have lawyers and technicians agree on a single definition).

In short, working definitions of 'ID-related crime' and 'ID fraud', and perhaps of other terms, should be developed that can be used in interdisciplinary discussions – not necessarily single definitions, but at least definitions that cover the various elements that are relevant to the context in which they will be used, and that are understood – if not necessarily agreed upon – by people from different fields and disciplines.

7.2 Towards combating the same thing

Once we know better that we are talking about the same thing – let us call it ID-related crime for now, and focus in particular on ID fraud with as primary elements unlawfully creating and using an ID – the next step is trying to combat this thing. It is clear that ID-related crime has a large impact on society, particularly as the information society is relying more and more on IDM systems in ever increasing applications, and we therefore take it for granted that efforts should be made to combat this. What ingredients should we at least envision?

7.2.1 Legal measures

The conclusion of Chapter 3 suggests that the problem is not so much a lack of legal provisions, far from it. It is more the lack of enforcement and absence of a comprehensive legal framework that are bottlenecks. Nevertheless, in some countries, certain gaps may exist that make it harder to effectively prosecute ID fraudsters, and hence, the details of criminal provisions may be improved. More important, however, is the need for enforcement and developing a legal framework that takes into account all the complex and multi-faceted

aspects of ID fraud. It is clear that 'the law' cannot do this on its own, but that input is needed from other disciplines.

7.2.2 Social-economic measures

Chapter 4 noted that, whereas figures on the incidence of ID fraud are abound in the US, European figures are scarce. There may be a large 'dark number' of ID-related crimes that do not show up in crime statistics, for one thing because the term 'ID-related crime' is not used as a separate category. Empirical research on the incidence and gravity of ID fraud seems urgently needed in this light.

Apart from empirical research on the incidence of ID fraud, other social-scientific research is needed, for instance, on the way in which IDM systems are used in practice and which human or organisational aspects create vulnerabilities. After all, technical security measures are important to make ID fraud as difficult as possible, but if these measures do not go well with the way people in real life want to use ID systems, then there is a risk that less secure systems will continue to be used, or that people will find tricks to by-pass the technical security measures (for example, telling a password to their secretary).

7.2.3 Technical measures

A lot of research is being done on the technical security of IDM systems, and this is obviously a key instrument in combating ID fraud. Promising technologies are being developed, with a lot of attention being paid to biometrics. As chapter 5 shows, however, biometrics are by all means not intrinsically secure, and so, ID fraud will not necessarily be effectively combated just by implementing biometrics.

Moreover, IDM systems do not function in a vacuum but in a context of cultural, organisational, and legal norms and practices, which may differ from country to country, even within the European Union. Research on ID fraud prevention must therefore combine at least technical and social perspectives.

7.2.4 The right mix of measures

At the core of combating ID fraud lies a combination of technical, organisational and socio-economic, and legal measures, and perhaps of other measures as well. The key question, we think, is how to determine the right combination of all these measures. Which efforts should be made in prevention, and which combination is needed of technical security measures and other efforts to prevent ID fraud, such as education, standardisation or tax measures? And how much effort should be devoted to detection and punishment of ID fraud, given that prevention can and will never be a 100% successful? How can detection and punishment best take place: through self-regulation, through civil-liability measures, or through policing and criminal prosecution? And can that be achieved at the national level (which is inappropriate to combat large-scale cross-border fraud, e.g., through Internet phishing) or at the international

level (where mutual agreements usually take years to reach, and where cultural differences may easily block global efforts to harmonise legal approaches)?

These questions call for answers – answers that can only be given when experts from the legal, socio-economic, and technical fields co-operate on a common ground of ID-related crime research.

8 References

Acquisti, A., (2002). *Privacy and Security of Personal Information: Economic Incentives and Technological Solutions*, SIMS Workshop on Economics and Information Security, May 2002.

Anderson, R. (2001). *Why information security is hard – An economic perspective*, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf

Baecker, D. (1999). *Organisation als System;* Suhrkamp, Frankfurt am Main.
Ben-Ner, A. and Putterman, L. (2002). *Trust in the New Economy*, HRRI Working Paper 11-02, University of Minnesota, Industrial Relations Centre

Brickell, Ernest F., Jan Camenisch, Liqun Chen (2004). Direct anonymous attestation. ACM Conference on Computer and Communications Security, pp 132-145

Camenisch, Jan, Anna Lysyanskaya (2001). An Efficient System for Non-transferable, Anonymous Credentials with Optional Anonymity Revocation. EUROCRYPT, pp. 93-118

Camenisch, Jan, Anna Lysyanskaya (2000). Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation, Research Report RZ 3295 (#93341), IBM Research, November 2000.

Camenisch, Jan, Els Van Herreweghen (2002). Design and implementation of the idemix anonymous credential system. ACM Conference on Computer and communications, Security, pp. 21-30

Cate, F. H. and Staten, M. E. (1999). *Putting people first: Consumer benefits of information sharing*, National Retail Foundation.

CIFAS, (2004). *CIFAS – The UK's Fraud Prevention Service*, Brussels, EU Forum for the Prevention of Organised Crime, 2 February 2004.

Chapman, T. (2004). *Credit Reporting, Identity Theft and Privacy: Truth and Consequences*, Equifax Inc. Atlanta, Georgia, April 7, 2004

David Chaum (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, *Communications of the ACM*, 24/2, pp 84-88.

Chaum, David (1985). Security without Identification: Transaction Systems to make Big Brother Obsolete, *Communications of the ACM*, 28/10, pp 1030-1044.

Chaum, David (1990). Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; *Auscrypt '90*, LNCS 453, Springer, Berlin, pp 246-264.

Clarke, R. (1997). *Chip-based ID: promise or peril*. Proc. International conference on Privacy. Montrel, September, 1997. This paper is available at http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html

DIN 31000 (1979). DIN 31000 (VDE 1000): 1979-03 *Allgemeine Leitsätze für das Sicherheitsgerichtete Gestalten technischer Erzeugnisse.* DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE.

Ellison, C., Schneier, B. (2000). Ten Risk of PKI: What You're Not Being Told About Public Key Infrastructure, *Computer Security Journal*, vol. 16 (1), pp 1-7, See http://www.schneier.com/paper-pki.pdf

Elston, M.J., Stein, S.A. (2002), *International cooperation in on-line identity theft investigations: a hopeful future but a frustrating present*, see www.isrcl.org/Papers/Elston%20and%20Stein.pdf.

Federal Trade Commission, (2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace*, May 2000 http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Freyssinet, E. (2004). *IT Forensic analyses & identity issues*. Internal FIDIS workshop on Identity & Crime. IPTS organization. Fontainebleau, December 9th, 2004.

Frosch-Wilke, D. (2001). *Are e-privacy and e-commerce a contradiction in terms? - an economic examination*, Informing Science - Challenges to Informing Clients.

FTC (2005). *National and State Trends in Fraud & Identity Theft*, Federal Trade Commission, February 2005.

Freud, S. (1978). *Das Ich und das Es und andere metapsychologische Schriften;* Fischer, Frankfurt am Main

Grijpink, J. (2003). Identiteitsfraude als uitdaging voor de rechtstaat [Identity Fraud as a Challenge to the Rule of Law], *Privacy & Informatie*, August 2003, pp 148ff. [translation of the definition: Bert-Jaap Koops]

Gordon, G.R., Willox, N.A. (2003). *Identity Fraud: A Critical National and Global Threat*, Utica; www.lexisnexis.com/presscenter/hottopics/ECIReportFINAL.pdf.

ITRC, (2003). *Identity theft: THE AFTERMATH 2003*, Identity Theft Resource Center, Summer 2003.

Kent, S.T., Millett, L.I. (ed.) (2001). *Who goes there? Authentication through the Lens of Privacy,* Washington, D.C., pp 80-103.

Kieserling, A. (2000). *Kommunikation unter Anwesenden – Studien über Interaktions-systeme;* Frankfurt am Main.

Tadayoshi Kohno, Andre Broido, K.C. Claffy (2005). Remote Physical Device Fingerprinting, *IEEE Transactions on Dependable and Secure Computing*, 2 (2), April 2005, pp 93-108.

Levi, M. (2004). *The Social Impact of ID Theft/Fraud: Challenges & Responsibilities*, Brussels, EU Forum for the Prevention of Organised Crime, 2 February 2004.

Lindlau, D. (1987). *Der Mob: Recherchen zum organisierten Verbrechen,* pp 43-47, Verlag Hoffmann und Kampe, Hamburg.

Linnartz, J.P., Tuyls, P. (2003). *New shielding functions to enhance privacy and prevent misuse of biometric templates*, 4th International Conference on Audio-and Video-Based Biometric Person Authentication.

Litan, A (2004). *Phishing Victims Likely Will Suffer Identity Theft Fraud,* Gartner Analyst Report,

Luhmann, N. (1991). Die Form 'Person', in: *Soziale Welt;* 42. Jg., Heft 2, p. 167-175.

Luhmann, N. (1997). *Die Gesellschaft der Gesellschaft;* 1st Edition; Suhrkamp, Frankfurt am Main.

Luhmann, N. (2000). *Organisation und Entscheidung;* 1st Edition; Westdeutscher Verlag, Opladen/Wiesbaden.

Mead, G.H. (1934). *Mind, Self and Society,* Chicago Press.

Matsumoto, T et. al. (2002). Impact of Artificial 'Gummy' Fingers on Fingerprint Systems, *Proceedings of SPIE*, Vol. 4677, January 2002

Menezes, Alfred J., Paul C. van Oorschot, Scott A. Vanstone (1997). *Handbook of Applied Cryptography*, CRC Press.

Mitchison, N., Wilikens, M., Breitbach, L., Urry, R., and Portesi, S. (2004). *Identity Theft - A Discussion Paper,* Technical Report EUR 21098 EN, European Commission - Joint Research Center.

Perl, M. (2003). It's Not Always About the Money: Why the State Identity Theft Laws Fail To Adequately Address Criminal Record Identity Theft, *Journal of Criminal Law and Criminology*, Fall 2003, p. 169-208.

Pfitzmann, Andreas (2005). *Security in IT Networks: Multilateral Security in Distributed and by Distributed Systems*, Script; Dresden, http://dud.inf.tu-dresden.de/~pfitza/SecCryptI_II.pdf

Pfitzmann, Andreas, Marit Hansen (2006). *Unobservability, and Pseudonymity - A Proposal for Terminology*, Version 0.27 at http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.27.pdf.

Potter E.J. (2002). Customer Authentication: The Evolution of Signature Verification in Financial Institutions, *Journal of Economic Crime Management*, Volume 1, Issue 1, Summer 2002.

Putte, Ton van der, Keuning, Jeroen (2000). Biometrical fingerprint recognition: don't get your fingers burned, *Proc. IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications*, Kluwer Academic Publishers, pp 289-303.

Rabin, M. and O'Donoghue, T. (2000). The Economics of Immediate Gratification, *Journal of Behavioral Decision Making*, 13(2), 233-250.

Ruuskanen, J.P. (2000). *"Javacard"*, Seminar 'Jini and Advanced Features of Java' at the department of computer science, University of Helsinki. This communication is available at www.cs.helsinki.fi/u/campa/teaching/ruuskanen-final.pdf

Sood, K. (2004). *The UK Experience – What Measures are being taken and considered to combat identity fraud?*, Brussels, EU Forum for the Prevention of Organised Crime, 2 February 2004.

Stubblebine, Stuart & Paul Syverson (2000). *Authentic Attributes with Fine-Grained Anonymity Protection*; Financial Cryptography, LNCS Series, Springer, Berlin.

Synovate, (2003). *Identity Theft Survey Report.*, Technical report, Federal Trade Commission.

Thalheim, L., J. Krissler (2002). Body Check: Biometric Access Protection Devices and their Programs Put to the Test, *CT Magazine*, November 2002.

Tiné, S. (2004). *Identity theft: a new threat for civil society*, Brussels, EU Forum for the Prevention of Organised Crime, 2 February 2004.

UK Cabinet Office (2002). *Identity Fraud: a Study*, London.

Willox, N.A. (2000). *Identity Theft: Authentication As A Solution*, National Fraud Center, Inc. March 2000

Wright, T. (1994). *Privacy Protection Makes Good Business Sense,* Technical report, Information and Privacy Commissioner/Ontario.

Zuccato, A. (2004a). Holistic security requirement engineering for electronic commerce, *Computers & Security*, vol 23, issue 1, pp 63 - 76.

Zuccato, A. (2004b). Introducing privacy risks in a companies information system security risk analysis, In Duquenoy, P., Fischer-Hübner, S., Holvast, J., Rasmussen, L., and Zuccato, A., (eds), *Proceeding for IFIP Summer School "Risk and Challenges of the Network Society". IFIP WG 9.2, 9.6/11.7*.

9 Annex

9.1 Index of Tables

Table 1. ID Law Survey summary (as of May 2005) 31
Table 2. Mapping ID crime provisions on the ID frauds sequence 37
Table 3. Social functional systems 45
Table 4. Identity theft records. 62
Table 5. Incidence of ID theft as reported in the Synovate 2003 study for the FTC. 64
Table 6. Fraudulent reuses of identity information in the US in 2004. 65
Table 7. Estimates of identity fraud in the UK, USA and Canada 70
Table 8. Costs of ID theft in 2002/2003. 71
Table 9. Decomposing ID-related crime. 107

9.2 Index of Figures

Figure 1. ID fraud sequence, taken from Mitchison (2004, p. 21) 14
Figure 2. Phishing example impersonating CitiBank. 20
Figure 3. Sniffing example. 22
Figure 4. Introduced terms and their relationship 56
Figure 5. Requirement engineering process 74
Figure 6. Authentication of a Human by an IT System. 80
Figure 7. Authentication of an IT System by a Human. 82
Figure 8. Authentication procedures between persons and IT Systems. 83
Figure 9. Testing area of the scenario: The field of view and the human's walking direction are depicted. 87
Figure 10. Hardware equipment of the scenario. 87
Figure 11. Image of iris spoofed by low resolution print and also possibilities with fun lenses for enrolment and access control 90
Figure 12. Silicon casts of fingerprints with silicon cast negative and acrylate paint as positive. 91
Figure 13. Fingerprint access with copy of fingerprint on scanner "Digital Persona". 91
Figure 14. Keys managed by the TPM. 107
Figure 15. Use of pseudonyms certified by a Trusted Third Party and encrypted using the TPM 107
Figure 16. Sample taxonomy 107