DuD
Datenschutz und Datensicherheit

Forensic Implications of Identity Systems

Results from the FIDIS Report on Forensics

Zeno Geradts

With the use of new identity systems and devices, such as mobile communication networks and biometric devices, new forensic aspects are important: How do legal systems support the use of new evidence in court? And how reliable (e.g. tamper proof) are the devices and thus the extracted evidence?

Zeno Geradts

Forensic Scientist
Image Investigation and Biometrics
Department Digital Evidence of the NFI
www.forensischinstituut.nl, Ministry of Justice – the Netherlands
E-Mail: zeno@forensic.to

Introduction

In the FIDIS Deliverable 6.1 „Forensic Implications of Identity Management Systems" [GeSo06] an overview of the different forensic aspects and implications of Identity Management Systems is given. This work is mainly based on a joint FIDIS and European Network of Forensic Institutes (ENFSI) workshop (Krakow, September 2004) and thus includes input from a broad although not comprehensive range of partners. The focus here is on state-of-the-art technology; it does not attempt to be a comprehensive listing taking into account all Identity Management Systems.

In the document, a model has been derived as a basis to represent information pertaining to the forensic aspects of Identity Management Systems. This model is described in detail to highlight the key facets of this area. Additionally, using aspects of this model, the forensic implications of biometric systems and mobile devices, two case studies where forensic information can be extracted, are examined in depth. This document also describes a taxonomy concerning the different aspects of these systems related to forensic evidence in court, and gives an extensive overview of the impact of different legal systems on such „digital evidence".

1 Forensic properties

Challenges to Identity Management Systems could be mounted on several grounds of which the following are simply illustrations:

- that the artefact of identity document, token, biometric property magnetic-stripe card, smart-card, etc. – could be faked;
- that a legitimate artefact of identity could be obtained by fraudulent means;
- that a legitimate artefact of identity in the possession of its legitimate owner may contain misleading or inaccurate information;
- that there were fraud or poor quality procedures within the body issuing the artefact of identity such that it was unreliable.

2 Deriving a model of forensic aspects

Forensic scientists and investigators will generally look for material which exists but which was not necessarily designed to be retrieved and utilised as evidence. This material is termed „unintended audit trails", and for example could be: telecommunication records, cell site analysis; extended use of vehicle number plate recognition systems and so on. We have chosen a model as a basis to represent such information pertaining to the forensic aspects of Identity Management Systems:

1. an overview of the artefact;
2. the threat level;
3. forms of failure;
4. consequences of failure;
5. in conclusion: the forensic aspects.

Using this model as a basic framework, as an exemplary case study we shall examine mobile phone networks for their ability to provide reliable identifying information in the forensic context. Further, the use of biometrics as a unique identifier will be considered. Before going into depth on these issues, the legal aspects are important to consider, and should be taken into account depending on the court system that is applicable.

3 Legal aspects

3.1 Determining identity

The determination of identity is the principal aim of identity systems. In forensic science, the determination of identity can take the form of (1) establishing an identity of origin between two objects and (2) determining the nature of a specimen of evidence. The first category is typically the more significant one because it contributes to the final determination of the value of the evidence. It is, for example, more valuable to be able to say that two hairs belong to the same head, than to say that both hairs are human in origin.

The central task of the forensic investigator is to establish personal identity. Supplementary to this task is the identification of physical objects that may, in turn, contribute to the desired personal identification. Physical evidence can therefore be divided into biological and non-biological evidence. The advent of computers and the phenomenal growth of their use have given rise to a second category, apart from physical evidence, known as digital evidence.

3.2 Collecting evidence

An important question that needs to be answered is that of the legal admissibility of the evidence; one must first examine whether certain types or means of evidence are admissible or receivable. Two systems can be distinguished: (1) the system of the freedom of evidence, where the accent is put on the freedom of appreciation of the judge, and (2) the system of legality of the evidence, where the stress lays on the risks of judicial error or on the respect of the accused. Outside these two systems regimes exist where the evidence is even more restricted.

Since more terrorism-related cases have take place, the public outcry for better and more universally available identification technology has been significant and several countries have responded with legislation mandating not only better security but achieving that result using high-tech biometrics devices in airports and in immigration offices. While the risk of privacy infringement is still the most compelling argument against the widespread use of biometric technology in law enforcement, this view seems to hold less weight today, in light of the recent tragedies.

> However by using the biometric properties in an insecure way, the risk exists that the forensic value of a given biometrics is less identifying, since this property is known and can be copied from other databases[1].

The need for digital forensics training and laboratories is beginning to be recognised and met. Much effort and specialised training of law enforcement and forensic experts over the years have developed the process of preserving and analysing forensic evidence – fingerprinting, hair and blood analysis, DNA, ballistics, … – a process that criminal law has come to rely on today. Likewise, more training and resources are needed, especially in the form of more laboratories and research centres, for the practice of criminal law to benefit from electronic forensic evidence in the future.

> All this potential will only be valuable if prosecutors ensure law enforcement investigators and technical analysts follow the necessary protocols. In doing so, prosecutors can ensure that otherwise admissible electronic evidence is not suppressed or compromised legally either because of an illegal search and seizure or because the evidentiary foundation was not properly or credibly laid during trial.

The focus of most of the current legislation and judicial activity determines the admissibility of the evidence in broad terms. However, a clearer and universal legislative approach of the admissibility of forensic evidence could be of great importance, all the more keeping in mind the huge progress in the field of forensic science and its growing importance in the judicial world.

4 Mobile Phone Networks

In relation to the forensic aspects we found that the reliability of underlying technology differs for the services used: While SMS sender IDs can easily be spoofed, the cloning of a SIM card in order to use voice or data communication on another subscriber's account is much more difficult and even impossible if corresponding vulnerabilities of the technical infrastructure have been fixed by the network operator. Verifying with the operator which version of SIM-cards is used should allow to quantify the risk of SIM cloning in a particular case.

The relation of the ID artefact to an individual is judged as weak: This is particular true for pre-paid contract schemes where mobile network operators have no personal interest in the verification of subscriber identities. Subscriber data provided for forensic investigations therefore requires careful investigations in regards to reliability. For post-paid contract schemes the number of invoices paid to date will help to judge the risk of subscription fraud: Fraudulent accounts usually feature no paid invoices.

The criteria of audibility, transparency and disclosure cannot be answered in regards to the general character of this document: Signalling and billing data processing is usually customized to operator IT requirements and access therefore subject to individual policies.

> The length of data storing and concerns of ethical issues in using the data depend on local legislations. From a billing perspective data is usually only required for a maximum of six weeks (that's the usually monthly billing cycle plus two weeks for data processing), longer storing is usually only due to legal requirements.

5 Biometric Devices

In this part of the research several biometric systems were tested. The biometric systems are shown in Figure 1. It covers an iris scanner, several fingerprint scanners with different ways of acquisition (optical, ultrasonic, thermal, electro-optical, touchless) and an iris scanner.

In the experiments, tests were done with spoofing the fingerprints, the iris, hand scanners and a vein scanner.

Figure 1: Biometric devices tested

[1] FIDIS Deliverable 2.1 Inventory of Topics and Clusters, available at http://www.fidis.net/

Several methods concerning spoofing of fingerprints are described in literature. The most convenient method appeared to be the method that was described by Computer Chaos Club [St04] with printing the fingerprint on a transparent sheet using a laser printer, and making a cast of this fingerprint with wood glue (see Figure 2).

Figure 2: Spoof of a fingerprint with wood glue

With this method the optical fingerprint scanner was easy to use. Other scanners were more sensitive to dust and moisture. They were somewhat harder to spoof. We also developed own methods for spoofing such as a rubber stamp (even a real case with a PDA with fingerprint access is solved by using method) and using silicon casting material which is used in forensic toolmark examination as casting material.

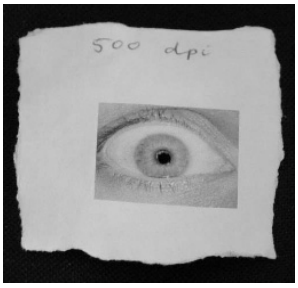

Figure 3: Copy of an iris with a hole

Also an iris for a consumer-grade iris-scanner could be spoofed with a picture with a hole as shown in Figure 3.

Figure 4: Spoof at hand scanner

With the security settings on low, a hand scanner could be spoofed with a 2D-copy of a hand as shown in Figure 4.

The vein scanner could only be spoofed when the liveness detection was turned off as is shown in Figure 5.

Figure 5: Spoof of veins in hand

It appeared that many biometric devices were easy to fool. The manufacturers' claims did not always appear to be accurate, which in later research appeared also to be true concerning the use of encryption on the signal over the USB-cable. Some of the tested scanners did not use any form of encryption, and with these devices it is easy to collect a database of fingerprints from the users.

> Concluding, it is evident that the current state of the art of biometric devices leaves much to be desired. A major deficit in the security that the devices offer is the absence of effective liveness detection. At this time, the devices tested require human supervision to be sure that no fake biometric is used to pass the system. This, however, negates some of the benefits these technologies potentially offer, such as high-throughput automated access control and remote authentication.

The independent testing of biometric devices is still non-trivial as manufacturers tend to sell their products for more than they can achieve. The latter can give a false sense of security, adversely affecting actual security if not recognised in time. It is an issue that we encounter in many forms of technology today: If it can be cracked, it will be cracked. Accepting this would need a different attitude of manufacturers, in which more of what is going on inside the device and the accompanying software is made public. It would allow potential users of biometric systems to better judge the fitness of such systems for their particular purposes.

From a forensic point of view, care should be taken when drawing conclusions from information extracted from access control systems that use biometric devices. The possibility that the system was compromised, consequently falsely linking persons to events, should be examined or at least noted in the forensic examination report.

Summary

The general conclusion that is drawn from this research is that evidence from identity based systems is legally permissible, and indeed heavily used in courts of law. For example, location information from Global System Mobile devices is frequently used for tracking individuals and subsequently for checking if associated statements made by suspects and witnesses with regard to their locations are correct. Similarly, supposedly unique biometric identifiers are becoming more frequently utilised to gain system access, and supposedly provide proof of a person's identity and thus accountability of subsequent actions.

However, with many of these systems there exists a possibility of incorrect association of a user with a mobile device, deliberate tampering with the system or system error through incorrect usage or technical faults. A classic example is that fingerprints can be spoofed, and indeed other biometric features can be copied, even without the owner of that feature knowing it. For this reason, in the examination process it is important to consider the likely integrity of the data, i.e. how failsafe the system is, since this could provide an alternative hypothesis, i.e. a different individual being involved in the crime. Equally, it is necessary to ensure law enforcement investigators and technical analysts follow the necessary protocols. In doing so, prosecutors can ensure that otherwise admissible electronic evidence is not suppressed or compromised legally either because of an illegal search and seizure or because the evidentiary foundation was not properly or credibly laid during trial.

References

GeSo06 Geradts, Z., Sommer, P. (Eds.), *FIDIS Deliverable D6.1 – Forensic Implications of Identity Management Systems*, Frankfurt a.M. 2006. Download: http://www.fidis.net/487.0.html

St04 Starbug, *How to fake fingerprints*, October 2004. Download: http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en