C24 Forensic Implications of Identity Management Systems

Zeno J. Geradts, PhD, Rikkert Zoun, MS, and Arnout Ruifrok, PhD, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, 2497 GB, Netherlands*

Through this presentation, attendees will learn what kind of evidence can be extracted from digital information management systems, such as mobile phones and their networks, and newer developments such as the biometric chip in the passport.

This presentation will impact the forensic community by showing the impact of identity management systems, such as biometric systems, for use as digital evidence.

Identification management systems are more widely used and are, in practice, useful for extracting forensic evidence based on the digital infor- mation. Examples of identification management systems, as defined within the European Network of Excellence, FIDIS, are based on artifacts, such as magnetic stripe cards, smart cards, biometric devices, mobile devices, RFID-tags, digital signatures, and many other tokens that are used. The systems for storing partial identities in databases or on cards are expanding rapidly (the biometric passport is an important example), and for forensic evidence it is important to know the forensic reliability of these systems, such as:

- reliability of the underlying technology
- how well is an individual bound to an ID artifact
- transparency and disclosure by manufacturer or government
- data protection issues, and admissibility of the evidence in court For reliable evidence in court it is important to know if:
- the central system could be misled, for example with compromise of communication channels
- a wrong person could be identified or not identified
- ease of data alteration and cloning

For mobile phones a wide use is available on extracting the data from the phones, and using location data as such. Forensic laboratories have developed tools to facilitate the examination of such phones. For mobile phones it is also known that particular SIM-cards could be misused by cloning them, and providers will improve the technology such that this kind of tampering is more difficult.

Another example of an artifact are biometric properties of a person. These biometric properties are acquired with a sensor. In this research, the authors have evaluated several technologies, based on expectation of future cases with biometric devices that could be misused. Different types of fin- gerprint readers have been acquired, with a wide range of sensor tech- nologies behind them, from optical scanners to ultrasonic. It is widely known that fingerprints can be spoofed with simple techniques using glue and a printer. Once someone's fingerprint has been copied, most of these systems can be tampered with. Often the manufacturers will claim that there is detection if a certain finger is alive. During experiments with the biometric devices tested, these kinds of protection are easy to tamper with. In the scanners tested the authors have not detected any indication of live ness detection.

Other biometric properties such as hand scanners, iris scanners, and vein scanners where also relatively easy to fake. The problem is that once there is a widespread use of these biometric properties, that the techniques to fake them will also evolve, and that the databases which store them could be compromised.

A good example of the practical implications of biometrics is the bio- metric passport. In the biometric passport, also fingerprint and face are stored in a contactless chip. The data is encrypted, and is not easy to change, however once the keys are available to the passports, it is possible to steal the biometric data without permission of the owner. Here also are a number of issues of the fall-back system if the system does not work anymore, and what the possibilities are of spoofing the system. With face recognition it is widely known that look-a-like fraud is easy to use.

For forensic examination it is important to be aware of the fact that the systems could be compromised. In case of doubt, other evidence should be combined with the digital traces (time line analysis and for example mobile phones with their location data), before drawing conclusions.

Biometrics, Identity Management, Taxonomy

 ** Presenting Author*