D17 Extracting Forensic Information From Biometric Devices

Zeno J. Geradts, PhD, NFI, Laan van Ypenburg 6, Den Haag, 2490 AA, Netherlands; and Arnout C. Ruifrok, PhD, and Jurrien Bijhold, PhD, NFI, Volmerlaan 17, Rijswijk, 2288 GD, Netherlands*

The goal of this presentation is to describe forensic information that can be extracted from biometric devices and methods for spoofing biometric devices.

This presentation will impact the forensic community and/or humanity by presenting an overview of the forensic value of data from biometric systems.

In the last decade, both industry and governments have started to contribute to ever larger projects on biometric devices. Terrorism has highlighted the need for better identification systems for people as well as 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. Biometric systems (especially fingerprint scanners) are mass-market products at low cost, and can easily be integrated in consumer electronics, like PDA's. Systems using fingerprints, iris, hand scans, and faces are commercially available and routinely used at e.g., airports.

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.'

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. 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.

The authors have tested several fingerprint systems and an iris system for possibilities of tampering, and it appeared to be easy if a person allowed to enroll into the system is cooperating. Some biometric features can also be copied without the person knowing that it has been collected (for example fingerprints).

Several other patents and information sources describe the method of computing a template used for the comparison. Depending on the implementation, it may be possible to reverse engineer the template, and try to compute a biometric feature. This way a biometric feature may be 'stolen,' and with it, identity theft may be committed.

It is clear from the above, that most biometric systems are not completely tamper-proof, especially if the equipment is unattended. When investigating evidence from biometric devices, the forensic examiner should consider the possibilities of tampering with the biometric systems, or the possibilities of unauthorized access, before drawing conclusions. If there are suspicions that someone tampers with a biometric system, one should look for e.g. silicon casts of hands or fingers, and examine log files of the biometric access devices. An overview of tampering with these systems shows how to enter biometric systems with photographs of faces, with copies of the fingerprints, with a contact lens for an iris system, or even using a latent fingerprint on the scanner, etc.

From a forensic perspective potentially even more information may be extracted from biometric databases. If the biometric data is stored in a database in a standardized way, it is possible to extract statistical data, and have more information on the uniqueness of biometric features.

Fingerprint, Biometrics, Tampering

 ** Presenting Author*