D8 Forensic Use of Biometric Access Devices

Zeno Geradts, PhD, and Jurrien Bijhold, PhD, Netherlands Forensic Institute, Volmerlaan 17, Rijswijk, The Netherlands*

The goals of this presentation are to **increase** awareness of forensic evidence from biometric access devices and methods of tampering with these devices that have to be taken into account before drawing conclusions.

Over the past few years, both large multinationals and governments have begun to contribute to even larger projects on biometric devices. Recent terrorist attacks in America and in other countries have highlighted the need for better identification systems for people as well as improved systems for controlling access to buildings. 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. The interface between the system and the user is routinely abused, as people have to remember many complex passwords and handle tokens of various types.

Many users fall prey to socially engineered attacks, or choose easy- to-guess passwords and then write them down. For the reason of security, biometric systems are used. Systems with fingerprints, iris, hand scans, and faces are commercially available and are also used at airports. Many other biometric data are under investigation for commercial systems, as ears, gait, keystroke, odor, etc.

Testing and comparison of biometric systems has been an issue. Comparison of algorithms used in facial recognition is undertaken in the FERET program. Often of more interest is the “real life” performance in a situation approximating that of future deployment. New suppliers are often tempted to make claims of excellent performance based upon a small laboratory test or mathematical simulations. In practice it appears that face systems are still not good enough for many applica- tions, since faces change in time, and they are difficult to acquire in a standardized way. New developments are in heat maps and thermo- grams, and developers claim that easier identification of individuals is possible. The BIOTEST project led by the National Physics Laboratory has produced a set of best practice guidelines for these systems that can be used for examining biometric systems. Also NIST is involved in developing standards for biometric systems.

The literature in this field is mostly focused on a well-engineered sensor, or the algorithms that are used. Less well-described are the systems of which biometric is a small part. If it is not integrated securely, or if the system is vulnerable to an unexpected attack, even the best device will be compromised. Often the biometric system compro- mises a smart card with data of the finger print or the iris scan which is compared with the data of the person that would like to have access.

For forensic evidence the biometric devices can be important, since more information is available of the person who tries to access a building or a computer. They may also be helpful in cases of hacking if a suspect has been logged on with biometric data (e.g., a fingerprint).

With biometric devices it is still possible to have unauthorized access. Depending on the chip card that is used, someone can tamper with the data. Furthermore, it is also possible to copy the data from a person (e.g., a silicon cast of a finger). The problem with spoofed biometric data is that they cannot be revoked and renewed, as would have been done with a stolen key. Another reason for unauthorized access is that there are false acceptance rates, depending on the settings of the biometric device. Often the setting of the biometric device will be changed to have less false rejects, and this might cause the system to fail. In practice, biometrics is not more secure than PINs. For this reason it is good to have a combination of biometric data and PINs for access.

In forensic evidence with biometric devices the forensic examiner should consider the possibilities of tampering with the biometric systems or the possibilities of unauthorized access before drawing conclusions.

Biometrics, Tampering, Fingerprints

 ** Presenting Author*