Robert Brumnik,
Iztok PODBREGAR,
Faculty of Criminal Justice and Security, Ljubljana, Slovenia

BIOMETRIC IMPLICATIONS ON THE FUTURE'S GLOBAL CRIMINALITY

Biometry, turning point in evolution of personal identification

Biometrics contributes a new dimension to authentication and identification process of persons. Besides knowledge (passwords) and possession (smart cards), biometrics provides new means of personal identification. Biometrics procedures are used to recognize or verify behavioral or physical characteristics of a person. Also biometry provides us with a user-friendly method for automatically identification and becoming a competitor for current identification systems, especially for electronic transactions. Cause of biometric increasing position in electronic transaction and security identification system we must to assure perfect information security tools to purpose stability such a systems.

But before deploying any security tools or system, one should carefully examine the sensibility and added value of it, as we do in our daily work. However, there are ways to compromise a system based on biometric identification. This article focuses on the future and draw-after of biometric identification, specifically implication on tomorrow's network society.

Key-words: *Identification, Authentication, Verification, Biometry, Electronic transactions, Security Systems, Network Society*

1. Evolution of personal identification

Such we can read in previous chapter biometrics are not really new technology. With evolution of computer science consecutive manner in which we can now use these unique features with computers aid is contemporaneousness. In future will modern computer aid biometrics technology plays a critical role in our society to assist questions related to the identity of individuals in global world.

2. Biometric dilemma – Crime of the future

Will the biometric methods when implemented actually make us safer? Can this sofisticated technology make us more secure? These are some of the questions that people should be asking themselves.

"Watch where you leave your fingerprints" – soon they could be the target of thieves looking to break into your bank account. Although in Europa biometric security systems using fingerprints, iris scans and facial recognition are just now entering the mainstream, but they are be common within a few years.

And as soon as biometrics begin to be used to protect bank accounts or benefit systems, crooks will start looking at ways of breaking into them. We are leaving our prints everywhere so the chance of someone lifting them and copying them is real. Over the past 10 years, crime has been moving away from stealing physical goods, towards obtaining information. First the means of robbery changed to keep up with an age where people carry identity information in the form of credit cards instead of cash. However, these are just the modern equivalents to common mugging.

One of the most worrying is the terrorists moving online, and engaging in what is called cyber-terrorism. These methods of producing destruction, terror, mayhem, and fear can be much more destructive online than other conventional methods in the real world.

What types exactly will depend on what new forms of security tomorrow's criminals will need to break. Will people be synthesizing voice authorizations? Or running replay attacks on retinal scanners? Or even learning to imitate a victim's typing style. All we can be sure of, is that criminals of tomorrow, like those of last century and those of today, will keep on innovating.

To avoid many malicious possibilitys it is today's research and development task to produce the crime-resistant products of the future. So we must take every opportunity we can to use science and technology to reduce crime and improve the quality of our lives.

2.1. Biometric spoofing

With developing of Biometric Tehnology we must aware that parallel Biometric spoofing become very sofisticated. Different biometrics

may be attacked in different ways. For example, researchers was successfully trick fingerprint systems with fake fingers made of gelatine in the past. Similarly, thieves could try to spoof facial recognition systems with photos, videos or facial disguises in order to get access to the systems or information they protect.

Currently it's only researchers that are doing spoofing and copying. It's not a mainstream activity – but it will be. It's just human nature; if it can be done it will be done if you can achieve some benefit from it.

Part of the problem is that many of the biometrics used by these systems are easily visible.

Many people are trying to consider biometrics as secret but we must to know they aren't. Our characteristics such as faces and irises are visible and our voices may be recorded. We left fingerprints and DNA everywhere we go and it's been proved that these are real threats.

To avoid such as spoofing biometric producers offer tighter security biometric systems – for example to check that a real iris is being presented rather than a photo or that a finger has a pulse.

2.2. Information Theft

With growing infirmation technnology usage there have been also growing number of cases of information theft over the past few years. While more and more electronic security measures have been going up to protect people's possessions and information, these new technologies have bugs and design flaws that are opening up whole new worlds for the technologically advanced criminal.

2.3. Criminal Identity theft

Identity theft occurs when a criminal uses another person's personal information to take on that person's identity. Identity theft is much more than misuse of a Social Security number-it can also include credit card and mail fraud.

2.4. Cyber Terrorism

A great deal of "cracks" are committed for the purposes of anarchy, humor, or as often stated by the perpetrators, "to be annoying." However, is this the mindset of a CyberTerrorist? Does he change an Internet web site to say a country's government is evil? Does he hack into a major corporation's voice mail system to make long distance calls? NO – that is not the domain of the CyberTerrorist – that is the domain of the amateur cracker community that exists worldwide.

A CyberTerrorist will disrupt the banks, the international financial transactions, the stock exchanges.

The key: the people of a country will lose all confidence in the economic system. Would a CyberTerrorist attempt to gain entry to the Federal Reserve building or equivalent? Unlikely, since arrest would be immediate. Furthermore, a large truck pulling along side the building would be noticed. However, in the case of the CyberTerrorist, the perpetrator is sitting on another continent while a nation's economic systems grind to a halt. Destabilization will be achieved.

3. How to avoid unexpected scenarios?

In order for a wide implementation of this technology, standards must be developed that will allow for their consistent use. The International Organization for Standards ISO/IEC JTC1 is the governing body of international biometric standards, but this standardization is still in progress. Also there are many International Standards such us ISO/IEC 19794-5 to define Image Quality Requirements and BS7799 covering ten major sections, each a different area as a Business Continuity Planning, System Access Control, System Development and Maintenance, Physical and Environmental Security, Compliance, Personnel Security, Security Organisation, Computer & Network Management, Asset Classification and Control, Security Policy to maximum protect Information System and personal informations.

In the future, fixed biometric standards will be in place to guide vendors and developers in the areas of biometric application profiles, interfaces, and system performance. Along with standardization there should be certain privacy issues addressed by law such as privacy and specific use guarantees as well as checks and balances to conduct audits to ensure compliance with these guarantees. This is a good reason that encryption and digitalization are recommended by leading industry organizations such as International Biometrics Industry Association (IBIA) and the BioAPI Consortium.

Literature and sources:

1. Balantič, Z., (2002): Multimedia in the service of prevention. 2nd International Conference on Occupational Risk Prevention (Gran Canaria Island, February 20th to 22nd, 2002., Barcelona, Escola Tecnica, Superior d'Enginyeria Industrial de Barcelona.
2. Hicklin, R. A., and Khanna, R, (2006): The Role of Data Quality in Biometric Systems
3. Jain, A. K., Bolle, R. and Pankanti S., (1999): BIOMETRICS: Personal Identification in Networked society, Kluwer Academic Publishers.
4. Janbandhu P.K. and Siyal M.Y., (2001): Novel biometric digital signatures for Internet-based
5. applications, Inf. Management and Computer Security, vol. 9.
6. Nadel, L., (2006), On the Future of Biometrics – Research, Applications, and Social
7. Challenges, IEEE CVPR 2006.
8. National Institute of Standards and Technology, Data Encryption Standard (DES), Federal
9. Information Processing Standards Publication 46-2, 1993.
10. Ratha N.K., Connell J.H., Bolle R.M., (2001): An analysis of minutiae matching strength,
11. Proc. 3rd AVBPA, Halmstad, Sweden,
12. Umut Uludag, Anil K. Jain, (2003): Multimedia Content Protection Via Biometrics-Based
13. Encryption International Conference on Multimedia and Expo (ICME 2003), Baltimore, Maryland, USA.

The article in the electronic journal:

14. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
15. National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.
16. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_71/lures_of_biometrics.ht
17. The Lures of Biometrics-The Internet Protocol Journal-Volume 7, Number 1-Cisco Systems, Danielyan, Edgar, Danielyan Consulting LLP
18. http://csrc.nist.gov/csor/
19. Computer Security Objects Register (CSOR)
20. http://www.blackwell-synergy.com
21. Langenderfer, Jeff and Linnhoff, Stefan: (2005), Journal of Consumer Affairs, The Emergence of Biometrics and Its Effect on Consumers.
22. http://www.riskmanagementmagazine.com.au/articles/FF/0C02DDFF.asp?Type=124&Category=1240
23. Cara Seymour, (2005), Biometrics: the future is now