Proceedings of the International Multiconference on
Computer Science and Information Technology, pp. 297 – 302

ISSN 1896-7094

Relationship between IT Security and users' needs

Adrian Kapczyński

Department of Computer science and Econometrics,
Silesian University of Technology,
44-100 Gliwice, Poland
a.kapczynski@polsl.pl

Abstract. This paper deals with mapping of IT security into users' needs. The scope of IT security domain was narrowed to authentication methods based on physiological or behavioral characteristics of human beings. Preferences of chosen group of people were diagnosed and based on that AI enhanced tool was built in order to help selection of biometric methods based on specified criteria.

1 Introduction

Contemporary IT solutions are based on policies among which those connected with security are treated as of utmost importance. According to B. Schneier the key area in IT security is authentication [6]. The process of verification of users' identity can be carried out basing on one or more factors: knowledge, possession and characteristics of human being. The latter factor is the fundamental of biometric methods and systems.

One of the key problems is the proper selection of biometric systems [1, 2, 4]. Most popular approach uses analysis of properties of biometric identifiers (like fingerprints, iris, retina, etc.). Empirical experiences show the simplicity of that approach and lack of taking into account other important issues.

Generally in the literature it can be found that biometric system is composed of functionally connected elements excluding from that the *human factor*. However J. Wayman and J. Ashbourn pay special attention to role of an user as and treat him a part of whole authentication process [1, 2].

Basing on the consulting experience of author of this paper it can be stated that the selection of biometric authentication system shall be based on analysis of specifications of biometric systems not (only) biometric identifiers. Mention analysis can be manual or computer-aided, but still based on rules. For the time being there is no computer based tool supporting process of selection of biometric authentication system.

The goal of the article is to build the methodology of selection of biometric authentication system based on analysis of users' needs and codification of created rules in knowledge base of an expert system.

In first chapter of the article the extended range of biometric identifiers was presented. As not all of presented identifiers are widely applied the market share of most popular methods (technologies) were depicted as well.

In the second chapter the characteristics of biometric methods were shown on so called Zephyr chart which presents 8 biometric methods in four aspects (criteria): cost, effort, distinctiveness and intrusiveness. That chart was built by biometric specialists without penetration of user's needs (some general needs were assumed).

In the third chapter the results of survey of user's preferences were shown as well as their visualization on a chart.

In the last part of the article the expert system built in order to support the selection process was briefly described.

2 Biometric identifiers

Biometric identifiers include the following characteristics [3, 4]:

- bitemarks,
- blood pulse,
- bone sound transmission,
- corneal surface topography,
- dental radiographs,
- dynamic facial features,
- dynamic Grip Recognition,
- ear canal feedback,
- ear geometry,
- EEG,
- eye movement,
- facial geometry,
- facial thermogram,
- finger wrinkles,
- fingerprint,
- gait dynamics,
- hand pressure profile,
- iris patterns,
- keystroke dynamics,
- knuckle creases,
- lip movement,
- mouse movement,
- nail patterns,
- reflection of acoustic waves in the head,
- retina patterns,
- signature dynamics,
- skin impedance,
- skin pattern recognition,
- smile recognition,
- vein patterns.

From presented identifiers only small number was relatively wide implemented in out-of-laboratory environments. The current state (2006) of market share was presented on Fig. 1.

As one can see the market in the year of 2006 is mainly taken by fingerprint biometrics. However as the time goes by the trends of growing share of iris and multiple biometrics can be observed [7].

In order to select set of biometric methods (or even particular one method) the criteria shall be chosen. IBG proposed four criteria: cost, effort, distinctiveness and intrusiveness. Those criteria were applied to build Zephyr chart which is presented in the next part of the paper.

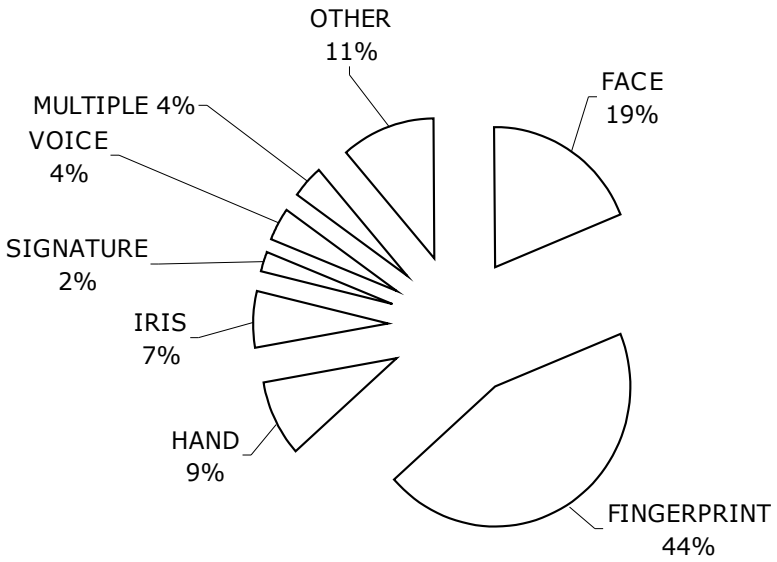

Fig. 1. International Biometric Group biometric market share (for 2006) [7]

3 Zephyr analysis

The most interesting result of Zephyr analysis provided by IBG is the chart of biometric technologies built by biometric specialists with assumed general needs of users. This chart shows the relation between ideal biometrics and most popular biometric technologies: iris, retina, voice, face, fingerprint, hand, keystroke and signature. Four criteria were applied and the result is shown on Fig. 2.

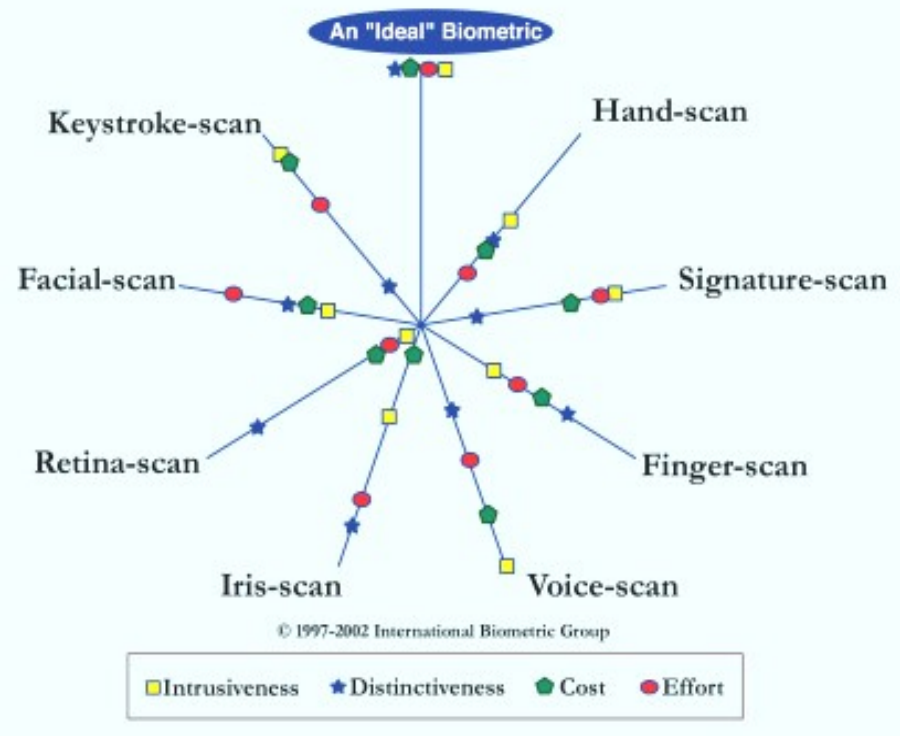

Fig. 2. International Biometric Group Zephyr chart [7].

This analysis does not take user expectations concerning strong authentication systems using biometric identifiers. Therefore new diagnosis of users' needs is requested.

In the next chapter the results of survey of user's preferences were presented as well as their visualization on a chart.

4 Diagnosing users' needs

In order to complement the system-oriented approach presented in previous part of the article the research using electronic poll was conducted. The poll included questions concerning the level of perceptive efficiency, convenience and acceptability of fingerprint, hand, voice, signature, iris and face biometric systems.

In total 100 fulfilled questionnaires were examined and the results were gathered in order to create the diagram of preferences of mentioned biometrics methods. The diagram does not include "cost" criteria because in this case it is considered as non-important and that is due to taken user-oriented approach.

The results of poll-research were gathered in tables 1, 2 and 3.

Table 1. Results of poll (1 of 3): Perceptive efficiency of biometric systems expressed in percentage of responses

Biometric / Note	Very low	Low	Medium	High	Very high
Fingerprint	3%	4%	6%	33%	54%
Hand	2%	3%	23%	53%	19%
Face	4%	7%	43%	29%	17%
Voice	5%	11%	24%	42%	18%
Iris	2%	8%	16%	33%	41%
Retina	7%	6%	25%	22%	40%
Signature	9%	22%	35%	24%	9%

Table 2. Results of poll (2 of 3): Perceptive convenience of biometric systems expressed in percentage of responses

Biometric / Note	Very low	Low	Medium	High	Very high
Fingerprint	3%	6%	8%	38%	45%
Hand	2%	5%	14%	36%	43%
Face	2%	13%	28%	27%	31%
Voice	2%	9%	22%	27%	40%
Iris	5%	13%	23%	38%	21%
Retina	6%	14%	25%	35%	20%
Signature	9%	11%	27%	23%	31%

Table 3. Results of poll (3 of 3): Perceptive acceptability of biometric systems expressed in percentage of responses

Biometric / Note	Very low	Low	Medium	High	Very high
Fingerprint	2%	3%	7%	31%	58%
Hand	1%	4%	16%	27%	52%
Face	2%	6%	33%	42%	17%
Voice	3%	8%	16%	35%	38%
Iris	3%	9%	20%	39%	29%
Retina	9%	14%	16%	32%	29%
Signature	3%	10%	23%	39%	25%

Given notes were assigned numeric values ranging from 1(very low) to 5 (very high). The average value for each biometric and each criterion was calculated by summing result of multiplication of numeric values and percentage of responses.

Basing on obtained results average values were calculated and presented in table 4.

Table 4. Average values of perceptive effiency, convenience and acceptability of given biometric method

Biometric / Note	Efficiency	Convenience	Acceptability
Fingerprint	4,32	4,15	4,43
Hand	3,85	4,14	4,25
Face	3,50	3,72	3,68
Voice	3,58	3,93	3,97
Iris	4,03	3,56	3,82
Retina	3,83	3,49	3,58
Signature	3,02	3,57	3,73

The values from table 4 were recalculated and scaled into range of [0;10]. These values were illustrated on Fig. 3.

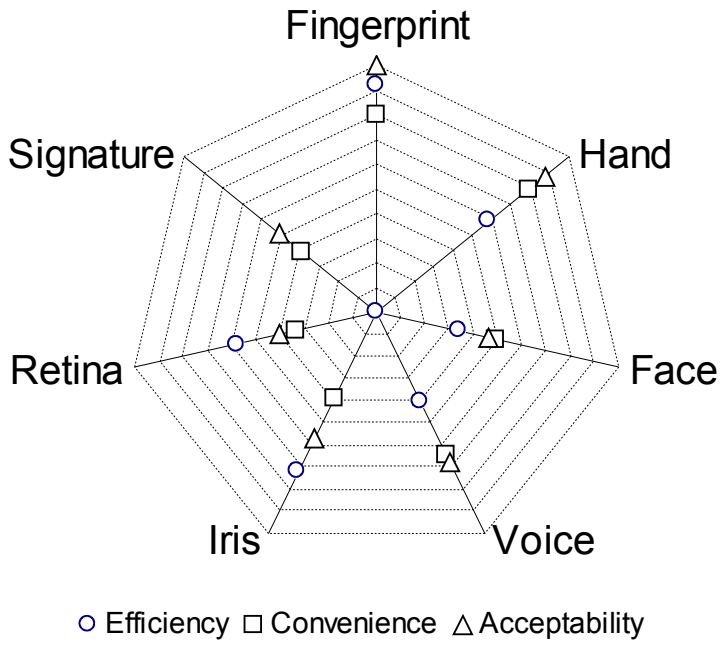

Fig. 3. Chart constructed using three criteria relevant in user-oriented approach

5 Expert system supporting biometric system selection

Obtained quantitative results were mapped into knowledge expressed in the form of rules, models and constraints written into rule-model expert system [5].

The solution consists of exact bases of: rules, models, constraints and advices. Implemented expert system during forward chaining queries the user to obtain values of askable arguments needed to proceed with the inference process.

In the output the set of biometric systems are proposed for further consideration.

6 Conclusions

This paper deals with mapping of IT security into users' needs. The scope of IT security domain was narrowed to authentication methods based on physiological or behavioral characteristics of human beings. Preferences of group of 100 people were diagnosed. The latter was the fundamental of knowledge base of expert system built in order to help selection of biometric methods based on specified criteria.

The emerging problem is to deal with values expressed in natural language which are uncertain or incomplete. This functionality can be provided by utilization of fuzzy logic theory created by prof. Lofti Zadeh which will become the basis for further research work in this domain.

References

1. Ashbourn J.: *BANTAM,* Springer Verlag, London (2002).
2. Ashbourn J.: *Biometrics – advanced identity verification,* Springer Verlag (2000).
3. Daugman J. G.: *High Confidence Visual Recognition of Persons by a Test of Statistical Independence,* IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. **15**, no. 11 (1993).
4. Nanavanti S., Thieme M., Nanavati R.: *Biometrics - identity verification,* Wiley & Sons, Inc. (2002).
5. Niederlinski A.: *Rule- and Model Based Expert Systems,* Pracownia Komputerowa Jacka Skalmierskiego (2006).
6. Schneier B.: *The importance of authentication,* Cryptogram 2 (2003).
7. Internet: *International Biometric Group,* `http://www.biometricgroup.com`