The Influence of Increasing Security Systems and the Destruction of Privacy

Miroslav Bača, Markus Schatten*

ABSTRACT. The strong development of information and communication technology (ICT) as well as the fact that there are currently over 800 million on-line users worldwide, bring us to the position of rethinking carefully about where all this data is going. Sending and receiving secure data is a well known concept. But what about data in the "open space" where everyone who knows how and has adequate technology can intercept or eavedrop our data and use it against us, to harm us or our family or to destroy the organization where we working in. The traditional answer to these influences is the development of strong security mechanisms and systems which will be able to protect us (in most cases) from our self and from others as well. Such security systems have the possibility to monitor all communication between users in a specific network or subnet and collect all information exchanged between them. And this is what we see as the main problem. Someone who monitors the system has access to all information about the network's users and can take advantage of these data as he pleases. This means that someone allways has full access to all private user data. Herein we introduce some ways of protecting users from legally monitoring of their private data.

Key Words. security, privacy, open systems, protection, cancellable biometrics

1 Introduction

In a situation where there is no strict law about computer security and data protection, the potential victims are unprotected. The most important law in the European Union (EU) is the Directive 95/46/EC of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995). According that Directive, most EU countries and membership canditate countries have to create and adopt their legislation. Secondly there is also the Directive from European Parliament of concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002). This recommendation tries to make order in everyday usage of electronic communication, especially in Internet and e-mail communication. And the last law important for this paper is Convention 108 (Council of Europe, 1981). In this Convention, the Council of Europe gives basic recommendations about protection of individuals. In this Convention we can find some basic privacy concepts regarding the protection of individuals that gives the necessary preconditions to use biometric systems.

These three recommendation laws establish the foundations for the development of a basic security system, but, there is no unique description of crucial terms like privacy and personal data. In (..., 1995) the lawmaker said that personal data *shall mean any information relating to an identified or identifiable natural person ('data subject'); an*

[*] Faculty of Organization and Informatics, University of Zagreb, Pavlinska 2, 42000 Varaždin, Croatia, {markus.schatten, miroslav.baca}@foi.hr

identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. In order to make it clear, layers used term sensitive and describe data like more or less sensitive for individuals privacy or deterring what is personal data. On the other hand, there is no punishment for people nor organizations that break these laws. For example, lawyers concur that someones name and family name is sensitive data which means that this data is personal and can compromise someones privacy or security. But, how many people have same name and family name? As an example, take the family name Horvat which is most popular in the north part of Croatia. We can assume that more then 50 000 citizens have this family name, and probably about 7000 citizens have the same name. So, we can't agree that someones name and family name is personal data. Why? There is no distinction between these 7000 citizens in their names and family names. If we can connect someones name, last name, street, house number, car etc. and from these data conclude what person we described this data we can be considered as personal data.

Today's most popular social networking application developed into a great opportunity for identity theft and the abuse of someones privacy or personal data. People usually don't think about such issues, but when it happens it's already too late for thinking. In a context of open communities which will use all benefits of ICT (which is a foundation for enhanced life quality) it is important to assure that every user has the right to know what is going on with his/her personal data and in which purpose this data will be used.

So, the major problem is how to use personal data in public services and protect them from unwanted usage. In the following a model that could address the stated issues concerning security without privacy destruction shall be presented.

2 What is important?

The most sensitive part distinguishing between sensitive and insensitive date, is the development of a unique model for data classification. Some research (Zhang et al., 2005) gives us a good base for it. In our proposed model we assume that only data that can uniquely identify a person is sensitive. Such data can be a social security number, other unique numbers of the person (e.g. driving license number etc.), as well as some biometric characteristics. Other types of data which can characterize a person but without additional data can't identify the person, like first name, last name and/or street address, are considered to be less sensitive data. Such data can be used in order to describe a person but it can be combined with some other data that could lead to identification. And finally, the third and last category of data is data which are not sensitive at all. Such data can be freely used and in order to identify the person one would have to combine it with several different data types. Examples of such data include hair color, weight, occupation etc. Using this data we can describe a person but we can't identify it.

We used a definition of data privacy in which privacy is considered to be data security with data protection in good sense. Still, one of the first definitions of privacy (Culnan and Armstrong, 1999) was that the information privacy is the ability of the individual to control the terms under which personal information is acquired and used. These two definitions are very similar. Let's observe, for example, a medical records data of some person. If we see only medical data without health security number or persons name and family name, we have only general few assumptions about someones health. But when we connect this data with sensitive (more or less) personal data we have a different view, and we know much more than we usually want or have to. But this "visible" data about us is not only personal or private data that describes us. We put lots of electronic footprints detailing our behavior and preferences; for example our buying habits are easily profiled.

We can't say what this data is or isn't important, for someone who making forensic or criminal analytics all this data can be very important, but in everyday use maybe it isn't. For this paper we will use our classification.

3 Tools

To achieve a wanted level of privacy and personal data protection we will use biometric data. Biometrics or biometric identification refers to identifying an individual based on her or his distinguished characteristics. Biometrics is the science of identifying or verifying the identity of persons based on physical or behavioral characteristics. Physical biometrics, like fingerprint, hand geometry or iris, are characteristics generally measured (or sampled) at some point in time. On the other hand, behavioral biometrics like signature, voice or gait consist of the way some actions are carried out and extended over time (Bolle et al., 2003). A typical biometric system is depicted on figure 1.

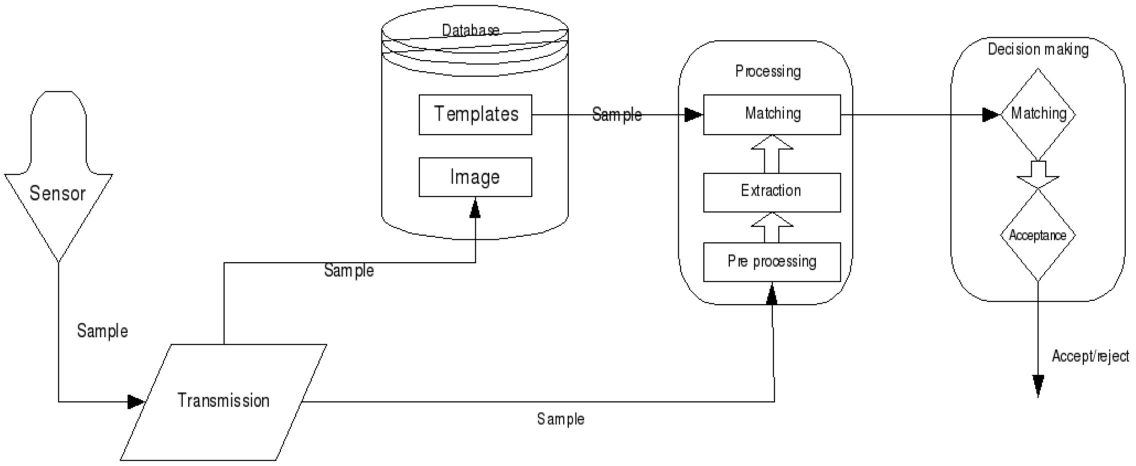

Figure 1: The main modules of a biometric system (source: Wayman (2000))

At this point, for this paper, the only important thing is the way of how to process biometric data. One of the problems with processing is the fact that biometric characteristics are most personal data. This is in a way like using the wolf to guard our sheep. But, as argued further, it is possible.

We will use biometric data for person identification (in a secure manner) and for the protection of personal and private data. To do so, we must use so called "hard" biometric data. Such data is unique for every person. The most obvious example are fingerprints. Why this data? This data is ideal for identification purposes, since such data is unique and there is no other person with the same data. If we use other characteristics (which aren't "hard") like voice, there is a probability that two persons have similar voices, which makes the distinction between them a hard task. The other reason is that it is much easier to develop cancelable biometric characteristics form "hard" ones. Cancelable biometrics is a concept in which biometric templates are transformed into a different form. But, in contrast to encrypted templates, they do not need to be transformed back into their original form before they can be matched to new samples for authentication purposes. In fact, for the transformation function we choose the one which is noninvertible, so that the template cannot be transformed back into its original form even if we want it to. The matching is performed by transforming the new acquired sample with the same transformation, and then making the comparison in transformed space (Bača et al., 2008).

This concept ensures that the original biometric template doesn't exist in the system. As such, it is not in danger of being exposed. The privacy issue is thus completely nonexistent. Even if an attacker is able to get to a transformed template it will be completely useless to him. He cannot use it to construct an artifact which could enable him to impersonate the original user. Even further, the template couldn't be used for identification purposes, like for instance law enforcement agencies use it to find a criminal. The existence of transformation functions allows simple control over which services have access and which haven't. The authorized services will have the knowledge of the transformation function, and the other will not. But this concept is not created only to address the privacy issues. The fact that the stored biometric templates are created by using a transformation function on the original biometric templates enables the creation of new templates by using a different transformation function on the original biometric templates of the user. If one can generate a new biometric template, the old one can be canceled. Biometric security systems which implement the concept of cancelable biometrics can enjoy all the benefits available in classic password based security systems (revocability and ability to reissue) but with preserving the benefits of biometric systems. Biometric templates are bound to the user so that they cannot be given to someone else. They cannot be stolen or forgotten. And they have a greater resilience to brute force attacks since they have a greater information space (Bača et al., 2008).

4 Model

The proposed model was developed, in the first place, for useage in a multimodal biometrics smart card environment and gave very good results from a practical perspective. The foundation of this model is the cancellable biometrics template which is the main input to the model. All users who have access to the database can freely use all data from the database without special approval, so where is the catch? All free data is non sensitive or less sensitive one. Sensitive data is encrypted by the given biometric characteristics in a so called biometric hash, and, in order to make all process more secure, we use cancellable biometric templates for the approval of using this data. The sensitive data owner must give her or his permission for its useage, otherwise, the data can be used but, nobody can connect it with the correct person. This way we make it possible to use all kind of data without special permissions, whereby the data owner is always protected from possible vulnerabilities.

Let's observe one typical example, health care. When patient come into the doctor's office she or he must give the doctor a smart card and do authentication through some biometric scanner. This way the patient allows the doctor to read all data from her or his database. The doctor can put some data about the patient into the smart card and/or into the database of the medical information system. If some other doctor wants to approach to specific patients data he must get approval of the patient using his or her biometric key. This biometric key is literally a part of the patient, so there is no way to get access to patients information if he or she isn't in physically present at the hospital.[1]

This approach can be implemented to all public services including government, tax paying, bank accounts etc. The most valuable advantage of this model is its adaptability to lots of situations, its protection of privacy, personal data protection and information security at the same time. The main problem of the proposed model includes practical issues concerning the acquiring and implementation of biometrics databases for all potential users.

[1] Here we presume the normal case, but off course there are ways to spoof biometric devices using death samples etc.

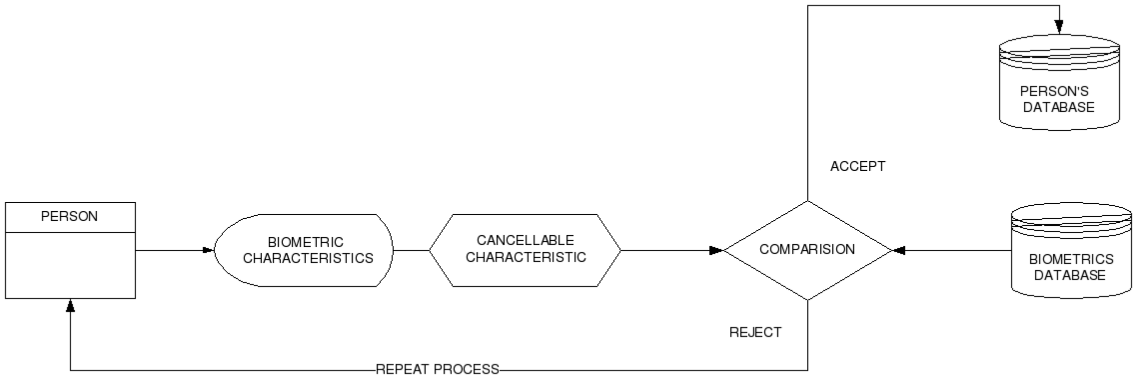

Figure 2: Prototype of Multimodal biometric smart card model

5 Conclusion

In this paper we presented a model for the protection of privacy and personal data. The model is based on using biometric characteristics in two perspectives: (1) as characteristics system authentication and (2) as characteristics for allowing the use of personal/private data. This model can opens several questions concerning the selection appropriate characteristics and as well as practical implementation issues. The most important factor as usual is user acceptance. If the user accepts using a biometric characteristic this model could give excellent results. Another open question is the development of an auto regulatory system for privacy and personal data protection. This system should address the privacy and security issues described in a social networking environment. We envision that such a system maybe be more adequate then the one we propose, but this kind of approach requires essential changes of user behavior and trust.

6 Future Work

For our future study we will try to use formalized knowledge in security and in data protection. If we imagine a common semantic wiki system where users can add formalized knowledge about known security issues on a particular platform certain intelligent agents could be developed. Such agents need to be able to analyze the semantic content on the wiki system with regard to the particular PC configuration, and common issues using the semantic content. On the other hand, malicious users could try to compromise the semantic wiki system, due to its openness, in order to do harm or gain access to users PC-s. To prevent such possibilities the use of potentially malicious formalized knowledge has to be minimized. To do so the social network has to be formalized with trust relations between users. Such trust relations will help in constructing a dynamic hierarchy of most trusted contributors with their respective trust-ranks.

References

..., 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Official Journal of the European Communities, Vol. L, 281, 31.

..., 2002. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the* *electronic communications sector (Directive on privacy and electronic communications).* Official Journal of the European Communities, Vol. L, 201, 37–47.

Bača, M., Antonić, M. and Magušić, F., 2008. *Upgrading Existing Biometric Security System by Implementing Concept of Cancellable Biometrics.* In B. Aurer and M. Bača (eds.) Conference Proceedings of the 19th Central European Conference on Information and Intelligent Systems. 421–426.

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K. and Senior, A.W., 2003. Guide to biometrics. Springer-Verlag, New York, USA.

Council of Europe, 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 108.* Signed 28 January 1981, entered into force 1 October 1985, `http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm`, (accessed: 21-02-2008).

Culnan, M.J. and Armstrong, P.K., 1999. *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.* Organization Science, Vol. 10, 1, 104–115.

Wayman, J.L., 2000. *Generalized Biometric Identification System Model.* In Collected Works 1997. - 2000., San Jose State University. 25–31.

Zhang, N., Wang, S. and Zhao, W., 2005. *A new scheme on privacy-preserving data classification.* In Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining. Chicago, Illinois, USA, 374–383.