ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2009. No. 7(95)*
ELEKTRONIKA IR ELEKTROTECHNIKA

ELECTRONICS
T170
ELEKTRONIKA

Biometric Techniques in Identity Management Systems

R. Volner
Department of Air Transport, Institute of Transport, Faculty of Mechanical Engineering, VŠB – Technical University of Ostrava, Dr. Malého 17, 701 00 Ostrava, e-mail: Rudolf.volner@vsb.cz

P. Boreš
Department of Circuit Theory, Faculty of Electrical Engineering, Czech Technical University in Prague, e-mail: bores@feld.cvut.cz

Introduction

As biometric technologies become more entrenched in the wide variety of applications that can benefit from positive human identity authentication, there is a growing interest in resolving some of the inherent difficulties with biometric systems. The techniques surrounding the use of multiple biometric concept combinations have often been cited as the solution, and significant research has been conducted to develop the concepts and to quantify the benefits. Experts in this field communicate these ideas and results, sometimes developing new expressions and terms needed to convey the findings.

In an attempt to promote clarity and understanding of the advances in multiple biometric combination systems, the following material provides a basis in the form of terminology, description of computational aspects, and a framework for describing the processing. Three hypothetical examples are provided to illus1rate the use of the terminology and concept in recognizably practical situations.

Biometric technology - the automated recognition of individuals using biological and behavioral traits - has been presented as a natural identity management tool that offers "greater security and convenience than traditional methods of personal recognition." Indeed, many existing government identity management systems employ biometrics to assure that each person has only one identity in the system and that only one person can access each identity. Historically, however, biometric technology has also been controversial, with many writers suggesting that biometrics invade privacy, that specific technologies have error rates unsuitable for large - scale applications, or that the techniques "are useful to organizations that regulate the individual, but of little use where the individual controls identification and authorization."

Here, I address these controversies by looking more deeply into the basic assumptions made in biometric recognition. I'll look at some example systems and delve into the differences between *personal identity* and *digital identity*. I'll conclude by discussing how those whose identity is managed with biometrics can manage biometric identity management.

Biometric attributes as verifiers

In 1970, IBM listed "three basic ways to identify a terminal user":

- By something he knows or memorizes.
- By something he carries.
- By a personal physical characteristic.

Biometric attributes are quite different from other forms of verification in several ways:

- Tokens, PINs, passwords, shared secrets, and numbers are proxies for the individuals that hold them. Systems that recognize these are attempting to recognize individuals indirectly, whereas biometrics uses the body as a proxy for the individual.
- The nonbiometric verifiers must match exactly. Because there is no permissible "within - class" variability, "close enough" isn't considered. A PIN isn't correct unless all the digits match. Passwords generally require that the user type with the correct case. On the other hand, an individual can't precisely repeat biometric verifiers because of changes in biology, behavior, and the collection environment.
- If security for the parties involved in an application depends on nontransference of authorizations, nonbiometric verifiers aren't as secure as biometric characteristics, which are more difficult, although not impossible, to give to another person.
- PINs, passwords, shared secrets, and numbers can be assigned to fictional persons, legal persons, and agents, allowing for actions on behalf of natural individuals. I can give my spouse my ATM card and PIN for bank deposits and withdrawals on my behalf, but not my iris pattern.
- System management knows and can control how much fundamental "between - class" variation exists between PIN or password verifiers, by using long

string length or assigned PINs, for instance. The fundamental variation in observed biometric verifiers across different populations and observations environments isn't well understood.
- System administrators can revoke or reissue tokens, PINs, and passwords. System policy might require the user to choose a new PIN every 60 days, for example. Biometric characteristics are fixed to the data subject.
- Tokens, PINs, and passwords can be application specific; biometric characteristics can't. Every application that requires my right thumbprint has access to that verifier.

As verifiers, biometric attributes have very different qualities and thus aren't transparently interchangeable with PINs, passwords, keys, and tokens. Each method has a different impact on security, privacy and usability.

Biometric attributes as identifiers

Some biometric measures are distinguishing and stable to the extent that identity management systems can use them as identifiers - the "attributes [which] serve principally to 'identify' you, that is to allow one to query (or 'index into') the database and retrieve some or all of your record," as the DSB describes. Biometrics can let me voluntarily retrieve my digital identities in applications promoting privacy, security, and convenience.

Biometrics' positive aspects are widely appreciated within the technical community, but fear of their negative implications on privacy has led to controversy. To deconstruct these controversies, let's examine the qualities required of "certain of the attributes [that] serve principally to 'identify' you."

In a 1973 report, the US Department of Health Education and Welfare (HEW) described qualities for an ideal *standard universal identifier* (SUI):

- *Uniqueness.* No more than one person can have the same SUI, and each person must have no more than one SUI.
- *Permanence*. It must not change during an individual's life.
- *Ubiquity*. The entire population must be issued SUIs.
- *Availability*. They must be readily obtainable or verifiable by anyone who needs them.
- *Indispensability*. Each person must remember his or her SUI and report it correctly.
- *Arbitrariness*. The SUI must not contain any information.
- *Brevity*. It must be as short as possible.
- *Reliability*. It must be constructed with a feature that detects errors.

Personal control over identity management

Governments and citizens might not always share the same perspectives on identity management, with citizens seeking to exercise some control over how their personal identity information is managed. We often label this desire as a privacy concern.

Privacy literature generally distinguishes at least two forms: intrinsic, or bodily, privacy, and informational privacy. Intrinsic privacy is encapsulated by the phrase "the right to be let alone," informational privacy by "the right to determine for ourselves when, how, and to what extent information about [us] is communicated to others." This taxonomy is now considered canonical in the literature, but examining my previous discussion on both personal and digital identity, we might question how much control I can reasonably maintain over both intrinsic and informational privacy when so much of my identity record depends on mutual extrinsic relationships.

Using biometrics in identity management systems involves both traditional forms of privacy. People might raise intrinsic privacy objections to biometrics' reductionism aspects, with its implicit definition of a person as a body, recoiling from the requirement for close bodily inspection and the equating of a person with flesh. Additionally, contact devices, such as fingerprint scanners and hand geometry readers, are no worse than doorknobs when it comes to harboring virulent bacteria, 18 but given that some people avoid hand contact with doorknobs in public restrooms, those people might also have intrinsic privacy objections to having to touch a public surface. Other biometric recognition techniques, such as iris and face imaging, can be done from a distance of several feet, so fewer people might object to using these noncontact devices. On the other hand, some users have religious or social objections to requirements that women expose their faces or wrists. Beyond the biometric component, people might have an emotional reaction to the reductionism in the words "digital identity" and "identity management," which seem to imply only the forensic, extrinsic meanings to the first - person concept of identity and that indicate that "I" can be managed by a technology.

Common concerns from the privacy advocacy community focus on informational privacy - the record linkages that system administrators might make from identifying attributes. Letting individuals maintain multiple identities (whether digital or not) within society lubricates social interaction. My work colleagues don't want to know about my religious and political affiliations, and my sporting friends aren't interested in the details of my work. An oft - noted problem with biometrics is that some attributes, even if collected as verifiers, can act as universal identifiers, allowing the data holders to link identity records. However, other forms of verifying attributes - what you have or know or what you are assigned - also share this problem. Cell phones, if turned on, indiscriminantly broadcast their identifier and location at frequent intervals, making them much easier to obtain than biometric measures; the biometrics community has frequently noted the irony of cell-phone users worrying about biometrics' privacy implications. On the other hand, cell-phone numbers aren't as permanent as biometric identifiers and could be replaced, perhaps several times, over a person's lifetime.

Example – a personal experience of biometric airport systems

The first indications show that the installation of such systems must be well prepared. In particular, the interface with the access control software and smartcard database

must be studied on a case-by-case basis taking into account the characteristics of each airport.
Interoperability with the automatic access control systems required an upgrade of the software to ensure a coherent exchange of information.

Regarding the ergonomic aspects, it should be noted that some manufacturers' recommendations did not give satisfactory results, in particular with regard to the position in height and slope of certain cameras. These simple elements can have a great influence on the rates of false rejections. Regarding the level of the lighting conditions and of contrast (for instance, a white screen behind the person) it was noted that if these conditions are not similar at the registration desk and on the checkpoint, then the false rejection rate could be much higher than expected. The correction of such a defect has to be undertaken very quickly to avoid the loss of confidence of the personnel in the techniques used.

From the sociological point of view, we noted a difference in the apprehension from technologies according to personnel categories. Facial or iris recognition seems more easily accepted than fingerprint recognition.

The experiments will now continue to measure the performance parameters of each piece of equipment. Very close attention will be paid to the evolution of these parameters according to the levels of sensitivity used.

For smooth operation and positive user experience, biometric systems must be integrated into the real world process that they're supposed to safeguard. Consider my user experience with the IRIS system at London Heathrow. Travelers are most likely to notice the system while queuing on arrival for immigration. As you stand there with nothing to do, you notice the occasional traveler breeze past in a separate lane, enter a glass box, and breeze out again. This suggests the possibility of improved efficiency and convenience. But to join the scheme, you must wait for your next trip: enrollment occurs in the departure lounge only, so you have to first plan and add sufficient time to your outbound journey, and then remember to drop by the enrollment office after passing through security.

The enrollment process itself was straightforward:

- First, a passport service official swiped my machine-readable passport through a reader.
- Then, I was directed to a desk, where I sat opposite a staff member with a PC and digital camera; under the camera was a screen facing me. The system captures both eyes, and I could see my face and target lines on the screen.
- Once my eyes had been captured, I was asked to look into the camera again, using the image on screen to guide me.
- Finally, I was handed a printout confirming my enrollment and passport data, and staff explained that I would have to walk up to the booth, look into a camera again, and wait for verification (a process that should, according to the UK Home Office Web site, take 20 seconds.) I received a paper slip confirming my enrollment and passport details and an "Arrival Guide" leaflet (see Fig. 1) that explains how to use the system.

The whole process took 7 minutes (there was no waiting time when I enrolled) and was free. My husband also enrolled successfully, with his glasses on.

Fig. 1. Arrival guide leaflet

Arriving back at Heathrow three weeks later on a red-eye, I headed for the IRIS booth, passing queues of other travelers. I faced a different interface from the one I had enrolled on: rather than sitting down and having the camera adjusted to me, I stood in front of three windows that, on closer inspection, turned out to be cameras. Depending on your height, the system determines which of the three cameras you should look into. Unless you're exactly the right height for the camera, you have to bend forward to bring your face into the camera's field of view. Once you see your face in the camera, you have to first move your face sideways to position one of your eyes in the target circles shown, and then move your whole body backward or forward to be at the correct distance. The resulting "bendy shuffle" can take some time. The system provides voice feedback, but it's general ("move forward/backward") and slow to arrive. Rather than assisting users in presenting their biometric feature, the system requires them to put their bodies in the right position. This is, unfortunately, typical for current camera-based systems for face and iris recognition. Systems with automatic height adjustment and auto focus are available and result in significantly better performance.

Conclusion

Biometrics has strong appeal in digital identity management, given that they can connect bodily people to identity records to create a one-to-one correspondence between people and records, restricting people to one record or records to one person.

These same qualities that make biometrics so powerful in identity management systems also raise very reasonable privacy concerns for the data subjects. Certainly, we must all place more emphasis on the importance of protecting our SUIs, including our biometric attributes, which, particularly if aggregated (by collecting multiple fingerprints or irises for every individual, for example),

can be at least as distinctive and identifying as SSNs and even more difficult to change.

To the extent that we caution people and enact laws to avoid unnecessarily disclosing our SSNs, so should we seek to protect biometric characteristics beyond merely encrypting stored biometric data. Rather, we should exercise discretion over who we give those measures to in the first place. The technical community should focus more on helping people manage identity management and their own biometrics.

References

1. **Prabhakar S., Pankanti S., Jain A. K.** Biometric Recognition: Security and Privacy Concerns // IEEE Security & Privacy. – 2003. – Vol. 1, No. 2. – P. 33–42.
2. **Watson A**. Biometrics: Easy to Steal, Hard to Regain Identity // Nature. – 2007. – Vol. 449. – P. 535.
3. **Harmonized Biometric Vocabulary.** ISO/IEC JTC1 SC37, standing document 2, version 8. – 2007.
4. **Volner R., Boreš P**. Aviation Data Networks // Electronics and Electrical Engineering. – Kaunas: Technologija, 2005. – No. 7(63). – P. 22–26.
5. **Volner R., Boreš P.** Multi-Biometric Techniques, Standards Activities and Experimenting // Electronics and Electrical Engineering. –Kaunas: Technologija, 2006. – No. 8(72). – P. 31–34.
6. **Volner R., Boreš P.** A Human Classification System for Biometric Parameters // Electronics and Electrical Engineering. – Kaunas: Technologija, 2005. – No. 6 (62). – P. 16–21.

Received 2009 03 17

R. Volner, P. Boreš. Biometric Techniques in Identity Management Systems // Electronics and Electrical Engineering – Kaunas: Technologija, 2009. – No. 7(95). – P. 55–58.

Biometric technologies have been suggested as a natural tool in identity management systems for enhancing privacy and assuring a one-to-one correspondence between people and records. But some commentators have questioned their value, saying biometrics are tools useful only for regulating individuals. The concepts of applying biometric techniques or devices to solve the practical problems that plague biometric deployments have been under development and ana1ysis for some time. The benefits promised include reduced error rates, better enrollment and higher levels of user acceptance. However, these benefits come at a cost, not necessarily the initial implementation costs, but also the investment in accumulating historical data for sensor characterization, development and tuning of computationally complex systems, and possibly in terms of user inconvenience and/or satisfaction. Ill. 1, bibl. 6 (in English, summaries in English, Russian and Lithuanian).

Р. Волнер, П. Бореш. Биометрические методы в системах проверки идентичности // Электроника и электротехника. – Каунас: Технология, 2009. – № 7(95). – С. 55–58.

Описываются новые биометрические устройства для определения личности. Излагаются способы уменьшения ошибок определения и увеличения возможностей регистрации параметров человека. Указано, что это увеличивает цену системы, однако значительно повышается вероятность точного определения. Ил. 1, библ. 6 (на английском языке; рефераты на английском, русском и литовском яз.).

R. Volner, P. Boreš. Tapatybės tikrinimo sistemose naudojami biometriniai metodai // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2009. – Nr. 7(95). – P. 55–58.

Biometrinės technologijos tapatybės tikrinimo sistemose padidina žmogaus privatumą ir asmenybės nustatymo tikslumą. Tačiau pasitaiko abejojančių, teigiančių, kad biometriniai įrankiai naudingi tik žmonėms valdyti. Jau kurį laiką kuriamos ir analizuojamos koncepcijos, kuriomis remiantis biometriniai metodai arba įrenginiai būtų pritaikomi kai kurioms biometrinės įrangos problemoms spręsti. Žadami tokie patobulinimai, kaip sumažintas klaidų skaičius, geresnės registravimo galimybės ir didesnis priimtinumas vartotojui. Tačiau įdiegus tokias funkcijas didėja kaina. Ją sudaro ne tik įrengimo sąnaudos, bet ir jutiklius apibūdinančių duomenų surinkimo, sudėtingų skaičiavimo sistemų tobulinimo ir derinimo išlaidos, taip pat jų priimtinumo vartotojui didinimo išlaidos. Il. 1, bibl. 6 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).