SECURE AUTHENTICATION COMBINED WITH ANONYMITY: THE END OF AN OXYMORON?

Evangelos D. Frangopoulos[1], Lucas M. Venter[2], Mariki M. Eloff[2]

[1] Electrical Engineer (M.Sc.) / Postgraduate Student, School of Computing, University of South Africa (UNISA).

215, Alexandras Ave., Athens, GR 11523, Greece.
Tel/Fax: +302106428483. eMail: vfrangopoulos@hol.gr

[2] School of Computing, University of South Africa (UNISA).

TvW 8 Theo van Wijk Building, UNISA, Muckleneuk Pretoria, South Africa.
Tel.: +27 12 429-6368. eMail: {ventelm,eloffmm}@unisa.ac.za

ABSTRACT

In a changing world where the global need for security through personal identification and authentication is becoming more prominent, the requirement for personal data to be kept private is of paramount importance.

This paper describes a concept for dissociating the notions of secure authentication and anonymity so that the two are no longer contradictory in the context of a security system or policy. This is achieved through the use of current state-of-the-art Smartcard technology and proposed advances to it.

KEYWORDS

Authentication, Security, Anonymity, Smartcard, Biometric.

SECURE AUTHENTICATION COMBINED WITH ANONYMITY: THE END OF AN OXYMORON?

1 INTRODUCTION

Although the world is progressively turning into the desired "Global Village", the necessary equilibria that used to hold together the closely-knitted village communities of yesteryear, can, merely, not be maintained on a global scale.

The escalating need for security in all forms and at all levels, calls for increasingly powerful security systems and the most stringent of security policies. Such systems and policies have traditionally been based on authentication and identification of subjects through the use of databases holding an extended amount of personal data.

Due to mounting serious security threats in recent years, it is becoming more easily acceptable to sacrifice an increasing part of one's rights to personal privacy, in order to achieve a heightened level of security and, thus, safety. In this context, anonymity becomes the first casualty.

The traditional way of authenticating a person is through the presentation of an ID card, passport, driver's license etc. In critical situations, such documents can be forged and the wrong person be granted access to a secure area or enjoy benefits normally reserved for the truly needy, such as special medical care. To be able to control forgery, technologies involving authentication and access through the use of special unforgeable tokens such as smartcards, have become popular over the past decade.

To further enhance security, the factor of biometric identification has also been added to the above schemes. Currently, systems employing such technologies require authenticating hosts that either obtain fresh biometric data from the person being authenticated and compare it against a central repository of authorised values, or against a reference value stored on an unforgeable smartcard that the person presents. In either case, a copy of the biometric data, together with some personal information of its owner is available to the host, and can hence be compromised.

Given the projected increase in the use of biometric data in the area of security and access control, it can be reasonable to assume that, in the foreseeable future, it will be commonplace for some kind of biometric property to be required to allow access to a house or apartment, as well as to grant use of one's own car, laptop, mobile phone etc. The idea that there will also exist repository databases where copies of everybody's biometric properties will be kept for security purposes, no matter how safe these will be claimed to be, simply does not seem acceptable. Such a repository can be compromised. After all, the existence of a totally safe system is, at least, utopic. In such a case, the biometric data which are compromised cannot be changed (as a password or PIN can be changed) and hence become worthless. Even if "cancellable biometric" techniques are employed, and only reference hashed values of

the original fingerprints are stored at the repository, a compromised authenticating host could lead to the compromise of the original, un-hashed fingerprint images. According to [3], the term "cancellable biometrics" refers to a technique "*where the biometric image is distorted in a repeatable but non-reversible manner before template generation, If the biometric is compromised, the distortion characteristics are changed, and the updated image is mapped to a new template which is used subsequently*". In effect, every time a person has to be authenticated through fingerprint matching, this technique produces a hash value of the freshly-acquired fingerprint image which is compared to the hash value of the reference image. A compromised host that performs the fingerprint capture and hashing outside the secure confines of the proposed smartcard, could be forced to release the fresh raw image once its hashed value is matched to the reference one. Thus, the raw fingerprint image could be rendered useless for subsequent secure authentication.

Thus, a scheme must be devised that will allow secure authentication of an individual based on biometric identification, at the same time protecting the privacy and anonymity of this individual as well as his/her unique biometric attributes.

2 THE BIOMETRICALLY-PROTECTED SMARTCARD

In [1], the case for a self-authenticating biometrically-protected smartcard was presented. In summary, such a smartcard is envisioned to employ all cryptographic controls in use by current technology smartcards along with a Personal Identification Number (PIN). Furthermore, a reference fingerprint value will be securely stored on the card and a miniature fingerprint scanner will also be incorporated on it, so that the user's fingerprint is scanned every time the card is used. Specialised fingerprint-matching software will be running on the card so that only a positive match between the freshly scanned fingerprint and the reference value will "unlock" the card and allow the authenticating process to proceed.

In [1] it is also shown that the different technologies required for such an implementation do exist, although some work is still needed before they are successfully combined to produce the proposed smartcard design. Furthermore, the need for an immediate expansion of the standards governing smartcards is discussed, in order to avoid arbitrary development of biometrically-protected smartcards, as it indeed happened in the early development stages of smartcards.

The interested reader is strongly encouraged to refer to [1] for a review of the current state of research and technology relevent to the proposed smartcard implementation.

A biometrically-protected smartcard such as the one described above is, in effect, a self-sufficient, stand-alone, authentication mechanism which ensures the identity of the bearer every time it is used. Its contents and integrity are cryptographically protected, thus ensuring that the card can not be copied, forged or tampered with. The scheme proposed in [1], apart from having a reference fingerprint value securely stored on the smartcard, also implements all of the fingerprint capture and matching functions on-card. Thus, any interaction of the smartcard mechanism with outside equipment is limited to cryptographically-protected "pass/fail" signalling.

Smartcards protected only by a PIN can be voluntarily given away or forced out of their rightful owner's possession (along with their PIN). They can thus not be

used as the only means of authentication of the bearer. In order to be certain of the identity of a user entering a protected perimeter etc, the smartcard will have to be used in conjunction to another form of ID or security token. This, to a large extent, defeats the purpose of having a smartcard in the first place.

On the contrary, a self-sufficient smartcard such as the one proposed, does away with more than one, security issues:

- The smartcard can not be used by anybody else other than its legitimate owner, whether the owner is willing to give it away or not. The smartcard requires its' owner's physical presence to function. Thus no other form of ID is necessary.
- A central repository of authorised users' biometric data is not needed and, thus, the risks involved in maintaining the security and integrity of such a system are nullified. The advantages that this scheme has from the standpoint of ensuring personal data protection against all risks, are obvious.
- The lack of a central database also has merit in the sense that authenticating stations do not need to be connected to it. Thus, the complexity of the system is kept at a minimum and the related vulnerabilities are eliminated.

The authenticating host / card-reader, is neither involved in the capture of fingerprint data nor in its comparison to a reference value. Thus, even if the authenticating host is compromised, the legitimate user's fingerprint value (which is part of the personal data that needs to be protected) can not be intercepted.

As far as the communication of the biometrically-protected smartcard with the authenticating host / card-reader is concerned, one point to be noted is that as a general protection against fake cards, standard encrypted-key techniques should be employed to authenticate the smartcard to the host/card-reader. These techniques are already in place in existing smartcard systems and the smartcard-authenticating process is totally transparent to the user. Parts 4, 8, 9 and 15 of ISO standard 7816 deal extensively with the security and cryptographic attributes of smartcards.

3 ELIMINATION OF THE CONTRADICTION BETWEEN AUTHENTICATION AND PRIVACY

Traditionally, authentication has been taking place through the presentation of a form of ID and comparison against a centrally maintained "exclusions" list. To guard against forgeries, biometric elements are currently being included in the proof-of-ID documents and the bearer of such a document is subjected to a biometric challenge every time the ID document is presented at control posts. Such authentication and identification methods can be used to generate a log of the individual's movements and actions. It is argued that the existence of such logs constitutes a compromise against the privacy of the individual. Furthermore, through the re-acquisition of the individual's biometric characteristics at every control post for authentication purposes, the possibility of those biometric characteristics being compromised, increases.

The most important feature of the biometrically-protected smartcard proposed in [1] is that being a self-contained mechanism, able to securely authenticate its user, it can be used in a way that separates the procedure of secure authentication from that of the identification of the card's legitimate owner by a third entity.

This separation is necessary if the privacy and anonymity of the card's legitimate owner are to be protected, while at the same time ensuring that the user belongs to a group of people who are authorised to enter a controlled perimeter or are entitled to receive certain benefits such as specialist medical care and administration of restricted or controlled medicine.

Furthermore, given that the biometric characteristics (fingerprints in this case) are not presented to any equipment that is external to the smartcard, the possibility of a compromise of those characteristics through an attack mounted against the external equipment, is drastically reduced if not eliminated altogether.

4 POSSIBLE APPLICATIONS

The authors believe that the possibilities for systems based on the discussed principle are limitless. A few examples may help to illustrate the point. The authors hope that these application examples will serve as food for thought and further research. They are by no means exhaustive descriptions of fully functional systems and despite the authors' efforts, there may well exist unresolved technical, legal and ethical issues. Further study of the proposed systems is highly encouraged.

4.1 The battle against AIDS

One possible application of such a system would be related to the very important treatment of HIV-positive patients. It would be advantageous to have HIV victims obtain the necessary special medicine such as AZT, while at the same time protect their privacy through anonymous, prescription-free, over-the-counter, dispensing of the medicine.

4.1.1 Overview of the proposed system

A system implementation through which such a scheme can be realised is as follows:

- Each patient receiving treatment will be issued one biometrically-protected smart card and a unique medical case identifying number.
- Each card will be personalised in the sense that it will be securely bound to the patient's fingerprint data.
- The card will hold:
    a) the patient's reference fingerprint value,
    b) a unique medical case identifier and
    c) a unique serial number identifying the card itself.
- The reference fingerprint value will not be kept anywhere else (such as a central biometric data repository, against which the case has already been made)
- To protect against multiple cards being issued to a single patient, it is deemed necessary to keep a database of the unique case-identifying numbers against a minimum set of patient-identifying personal details which does not include biometrics. In this manner, the same patient can not re-apply for a second smartcard unless the previous one is first returned to the issuing authority. Thus, workstations at the card-issuing authority sites will be the only ones in need of connection to the central database. Hence, the

possibility of that database being compromised is reduced by keeping the number of access nodes to a minimum. In the event of such a compromise, personal biometric data will not be placed in jeopardy.

- Once issued, the biometrically-protected smartcard will be used every time a new batch of the medicine is required.
- A log of previous medicine-dispensing transactions can be kept on the card, in order to prevent unnecessary dispensing of the medicine.
- Furthermore, the patient's medical history can also be stored on the card, making the patient's treatment more effective, irrespective of the medical facility the patient receives treatment in.
- Terminals at pharmacies, hospitals and health care facilities will not be able to read any patient-identifying details off the card because there will be none stored on it. These terminals will be self-sufficient, able only to read and update information on the card that is relevant to their function and will not be connected to a central database or upload transaction data to a repository.

It can not be stressed enough that the biometric data of patients can not be compromised because there is no central record of them. On the other hand, by design, the biometric data residing on the biometrically-protected smartcard will neither be accessible by terminal equipment interfacing to the card, nor through physical disassembly of the card. As far as the risk of the central database being compromised is concerned, any non-biometric personal identification data that is held in the database will be kept to a minimum.

Hence, the patient can be securely authenticated as in need of special medicine while the patient's anonymity is, at the same time, protected.

4.1.2 Loopholes and countermeasures

A possible loophole that may be exploited is if a card is falsely reported as lost or stolen, with the intention to be used by the authorised patient to obtain extra batches of medication. To control such fraud attempts, a black-list of smartcard serial numbers can be centrally created and kept. Each reportedly lost or stolen card's serial number will be inserted in the list, marking that card as revoked. The list will be downloaded at regular (e.g. weekly) intervals to the authenticating terminals in pharmacies, hospitals etc. Revoked cards will thus be swiftly identified and retained. Once they are returned to the issuing authority they can be destroyed and their serial numbers removed from the black list. An on-line connection of the authenticating terminals is not needed since the black-list updates can be simply downloaded at the predefined intervals over a phone line.

The black-list that is downloaded to the authenticating terminals only holds card serial numbers and not personal data. Thus, personal data can not be compromised if the terminal is compromised.

4.1.3 The case for HIV-positive illegal immigrants

If AIDS is to be controlled, all countries must provide all necessary medical services to all patients whether they are citizens or legal residents of the country in question, or not. In the past, attempts to provide such medical care and treatment to illegal immigrants were not successful because the patients would not turn up in hospitals and clinics out of fear that a police file on them would be created and deportation

would be imminent. Due to the seriousness of the spread of AIDS on a global scale, incentives must be given to AIDS patients who are illegally residing in a country, to actually visit hospitals and receive medical treatment. Preservation of their anonymity would prove to be the most important such incentive. Hence, the foundation can be laid for the effective and indiscriminate medical treatment of all HIV patients.

The proposed modification of the scheme already discussed, would be to provide illegal immigrants who are diagnosed as HIV-positive with a personalised smartcard without asking for any personal data that would identify them. The card will be personalised in the sense that it will be bound to the patient's fingerprint data at the time of its creation, and each patient will only receive a unique case-identifying number (which will, again, be digitally stored on their smartcard, along with their treatment history).

Under such a scheme, fraud that can involve multiple cards being issued to a single patient with the intention of obtaining large quantities of restricted or controlled medicine and diverting those into illegal sales' channels, must be prevented. Thus, in this case, a central database holding reference fingerprint values against the unique case-identifying numbers must be created. This database will hold biometric data relevant to illegal immigrants only and will only be consulted during the creation phase of a personalised patient smartcard. It can thus be established if a card has already been issued to the particular patient, by checking for a match to a fingerprint already in the database. Under such an implementation, only the card-issuing authorities will have to be connected on-line to the central database. In the event that this database is compromised, there will be no danger of personal data disclosure since there will be none recorded. The fingerprint values and case-identifying numbers will form the only data present in the database and will not be linked to any kind of patients' personal details. Hence, the privacy of the patient is, again, secured. (It goes without saying that revoked cards can be controlled using the same black-list principle described earlier).

Thus, it is also possible for illegal immigrant patients to retain full anonymity while being securely authenticated.

4.1.4 Controlling a possible loophole

The two variations of the smartcard system implementation that are presented above, lead to a serious loophole if employed simultaneously: A legal resident can get one card through the system requiring presentation of documents proving his ID and then posing as an illegal immigrant to the "no questions asked" fingerprint-only based system, get a second card. This, however, is not as simple as it sounds since the same person will be assigned two different unique case identification numbers that will have to be issued through two different hospitals. In order to retain those numbers, the person will have to undergo treatment at both institutions, something that is probably unfeasible in the long run.

On the other hand, there is no reason why the latter fingerprint-based system should not be extended to cover all patients, both legal residents and illegal immigrants, thus altogether eliminating the need for personal identification at the card-issuing stage.

As it was stressed earlier in this document, this is not an attempt to provide a fully detailed description of an application where every aspect is analysed and

resolved and it should only be seen in this light. However, the authors believe that it sufficiently demonstrates the ability to combine secure authentication with anonymity.

4.2 Measures against Hooligan actions

Another application of the proposed system would be in the fight against hooligan acts in stadia and sports fields during matches. Many countries around the world are attempting to control such acts by denying access to blacklisted fans. Fans are blacklisted on the basis of having committed acts of hooliganism in the past. Such people are, normally, denied access to sports events, by not having tickets or season cards issued to them. However, it is well known that a good percentage of people identified as hooligans always manage to get tickets and use them to gain access to events and cause trouble, even though these tickets are supposed to be personalised and controls at the gates are in place and functional. Furthermore, the control procedure is quite time-consuming, resulting in long queues and subjecting all the fans, the majority of whom are not hooligans, to long delays and frustration.

4.2.1 The biometrically-protected smartcard solution.

In an effort to expedite the control procedure and alleviate the frustration of non-hooligan fans, as well as provide a better means of blocking the access of hooligans to the games, an idea would be to allow fans who frequently attend sports events and who wish to do so, to be issued a personalised, biometrically-protected smartcard, which identifies them as "non-hooligans". This card will allow its holder to gain access to sports' events swiftly and securely without further ID checks. The card can be issued after the necessary documents are presented to the relevant card-issuing authority and be immediately personalised by storing the fan's reference fingerprint value on it. The card could have a limited validity period of a few months at a time, which is extended as long as the fan in question does not commit any offences related to hooliganism. The most important document for issuing or renewing the card would be a certificate issued by the competent state authority demonstrating that the fan has not been involved in acts of hooliganism. Since hooliganism is in most cases considered a crime, an entry is made in the offender's criminal record and as such, the said certificate would portray this. To have an access card issued or renewed, a recently issued such certificate would be required. It must be noted that in many countries, certificates of "blank criminal record" are required as a matter of course in many cases of transacting with the state and as such they are readily and easily produced.

In the system's basic form, a central repository of any kind of personal data will not be needed. The checkpoint terminals will not be connected to a central system and their only function will be to check the authenticity of the fans' smartcards by employing standard authentication techniques based on encrypted keys.

Such a system will allow speedy acceptance of fans to a match, based on secure criteria and will do away with the long queues and frustration involved in pre-match ID checks against a traditional black list. This is certain to function as a motive for the wide acceptance of the system by the fans, who in their majority, are not hooligans but who, up to now, are considered as such at checkpoints, until proven innocent! If this system is adopted, there will be two queues formed at checkpoints: a fast moving, smartcard-based one and another slow-moving one that will be based on traditional ID checking methods.

To avoid "Big Brother is Watching You"-type of concerns, although the card will be used to grant a fan access to an event, no personal data will be stored on it and as such, none can be disclosed every time the card is used. Furthermore, no record will be made of the holder of such a card attending the game (not even recording the identifying serial number of the card).

Hence, the card will be used to authenticate its owner as a member of a group of people who are allowed access inside a protected perimeter (the stadium or field) while at the same time the owner's anonymity and privacy will be preserved.

4.2.2 Exploiting loopholes in the system - countermeasures

Assuming that the documents presented at the smartcard-issuing centers are not forged, the only loophole in the proposed system has to do with the possibility of a non-hooligan fan who has been legitimately issued a smartcard, to be convicted for acts of hooliganism at a later point in time. The question is how to block the offender's further access to games through the described system. If the smartcard is found and confiscated at the time the suspect is apprehended after the game (at least until the legal procedure is completed and the suspect is found guilty), then, obviously, no problem exists. Assuming that the card can not be confiscated, the worst case scenario is that access to the games will not be blocked for the remainder of the offender's card's validity. This may still be acceptable if the cards are renewed on a three to six months' basis. Given that the main effort is to block hooligans' long term access to games, a short-term extension of access to someone who is charged or even convicted for hooliganism will not matter significantly. The offender will eventually be weeded out, probably in a manner more efficient than that of the current system of pre-game ID checks.

If the above reasoning is considered unacceptable, there is still a way to modify the system to cater for the need of immediate ban from games of legitimate smartcard-carrying fans who have turned into hooligans. This can be achieved through the creation of a central database that will only hold the identification details of fans against the unique serial numbers of the smartcards that are issued to them. Every time a fan is apprehended and charged with acts of hooliganism, his ID will be determined, and checked against the database to determine if a card has been issued to the said individual. If a match is found, the serial number of the card will be included in a black list (in a fashion similar to the one described in previous sections). The terminals used at pre-game checks will be updated with black-listed card serial numbers some time before the game or on a periodic basis. This can easily be done over a land or mobile phone line. Black-listed cards can thus be rejected and their bearers banned. As it was the case for the previous scenario, there will be no personal data on the smartcard and no record of the card's serial number will be made at the checkpoint. Thus, no "tracking" of the fans will take place.

Even in this case where a database is needed to correlate the card's serial number to the identity of the fan, there is no biometric data stored and the personal identification details of fans that need to be stored, will be kept at a minimum. Furthermore, the database itself is only accessible by the stations installed at the card issuing/renewal points and never by the authenticating terminals at game venue checkpoints. Hence, even if the database is compromised, there will be no significant concerns about a fan's privacy being transgressed upon.

In conclusion, the desired separation of secure authentication and identification is achieved, ensuring the anonymity of fans entering a stadium. At the same time, hooligans are not allowed to attend the games.

4.3 The fight against terrorism

With the onset of mounting global concern regarding terrorism after the September 11, 2001 hit in New York and following the attacks on Spanish trains on March 11, 2004, some hard-line schemes are being devised to ensure the protection of innocent civilians against terrorist attacks. Most of the schemes so far are based on the notion of checking out every single person entering an airport, train station, sea port etc. This is equivalent to "keeping tabs" on everybody so that everybody remains safe and secure.

Clearly moving in this direction, several countries are already creating extensive databases of visitors' personal data including their biometric properties (as is the case of the US and their US-VISIT policy [2]), or are involved in the process of creating the supporting legal framework to do so. Obviously, no one can guarantee the security of a central system holding this personal and -more importantly- biometric information, or provide any assurances that this information will be kept secret and that it will never be intercepted and subsequently used (perhaps in combination with other bits of personal details) to gain access to one's personal bank accounts, home security system etc. Although we are all willing to exchange some of our privacy for added protection against terrorism, there exist limits to such a compromise.

A system employing biometrically-protected smartcards used as "passes" that are issued after checking the individual's background (not unlike background controls carried out following an application for an entry visa to a country), may provide an optimal solution regarding security and access control, while at the same time minimising or even eliminating the infringement of a traveller's / visitor's privacy.

5 CONCLUSIONS

In this short paper, the viability of a system, based on a proposed biometrically-protected smartcard scheme, that can ascertain secure authentication while concurrently preserving anonymity and upholding the non-disclosure of personal data, has been demonstrated.

Systems following the discussed principles, combined with the proper underlying legal framework, can help protect the fundamental civilian right to privacy without compromising security.

The authors would like to thank the anonymous referees for their constructive comments and for drawing their attention to "cancellable biometrics".

6 REFERENCES

[1] E.D. Frangopoulos & L.M. Venter 2004. Biometric Protection of Smartcards through Fingerprint Matching: A Technological Overview and Possible Directions. In: *Peer-reviewed Proceedings of the Information Security South Africa (ISSA) Enabling Tomorrow Conference,* Johannesburg, 30/6 - 2/7/2004. (Available on CD (ISBN 1-86854-522-9) from the ISSA 2004 Conference Organising Committee at URL: http://www.infosecsa.co.za/)

[2] US-VISIT Privacy Policy Document, 2003. At URL:
http://www.dhs.gov/interweb/assetlibrary/USVISITPrivacyPolicy.pdf

[3] UK Government Information Assurance Technical Authority - UK Government Biometrics Working Group (BWG) 2003. Biometric Security Concerns. At URL:
http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricSecurityConcerns.pdf