E-Voting and Biometric Systems?

Sonja Hof

University of Linz, Austria
Institute of Applied Computer Science,
Division: Business, Administration and Society;
University of Linz, AUSTRIA
sonja.hof@ifs.uni-linz.ac.at

Abstract: As e-Voting gains more importance while practicable solutions are being implemented, more questions arise concerning alternative possibilities for a secure and feasible authentication. The specific peculiarities of secure authentication to a system are various and for a sensitive area like e-Voting also challenging. In this paper we evaluate biometric systems in order to prove their capabilities for e-Voting systems.

1 Introduction

This contribution tries to look into e-Voting from a different angle on the necessary citizen authorization from a different angle. Instead of concepts such as one-time passwords or smart cards, we try to look into the pros and cons of a biometric approach.

Biometrics is the science that tries to fetch human biological features with an automated machine either to authentication or identification [LA02]. Biometric products should remove the necessity of password or PINs. Typical two-factor authorizations use possession, e.g. smart card, and knowledge, e.g. PIN. Biometric systems try to exchange knowledge with an individual feature, e.g. finger print. Recording of the feature should be comfortable and fast. The most commonly use biometric feature is the finger print. It is well known and in wide spread use in daily police work.

In contrast to passwords or pin codes, biometric features are dynamic, i.e. they change over time. This is probably the most challenging property of the biometric system. One has to find a balance between a check which is too strict and generates too many rejections, and a check which is too loose and generates too many false accepts.

This paper gives an overview of biometric approaches to e-Voting. The first section gives an introduction into e-Voting. The second section elaborates on security issues specific to e-Voting systems. Finally, it focuses on security in e-Voting systems with biometric systems.

2 E-Voting

Many countries have started research projects or even pilots for e-Voting (UK [html5],[PKK03], ACM US [html6], NIST [html7], Austria [SM03], Switzerland [BR03],[html9],[html8], Germany [BR03]. There are two main motivations to introduce e-Voting: cost savings and increased voter participation and interest. Providing information and increasing the convenience for the citizens goes hand in hand, and it also offers disabled people the possibility to use e-Voting systems [html10]. Some approaches of putting e-Voting into practise are quite innovative, such as voting using SMS [html8] but still they have to cope with a lot of unsolved technical problems and therefore, it is doubtful if they will be implemented. The most sensitive aspects within e-Voting are fraught with secrecy and access issues.

3 E-Voting and Security

E-Voting is probably the most security sensitive process handled electronically nowadays [Cr02]. The main reason for this being that the worst-case scenario is really catastrophic. For example, assume an electronic vote for the German Bundestag is discovered to have been tampered with. This fraudulent act will not only have drastic consequences for Germany itself, but will also have enormous consequences for the whole European Union and further a field. Bearing this in mind, the highest achievable security is never too much for an e-Voting system.

Generally one can divide the requirements for an electronic vote into three basic musts:

- Do the actual laws in a given country allow for the electronic handling of votes?
- Does a technical solution exist that fulfils all the restrictions and requirements imposed on it by the corresponding laws?
- Do the actual voters desire and accept an electronic voting system and in particular, the designed voting system [Ba04] [Ev04]?

Fulfilling these requirements is quite challenge. Especially as their individual areas of expertise are different: law, technology and social science.

4 Biometric Identification in E-Voting

In this section, we will have a look at biometric systems [Zi03] focusing on their relevance for e-Voting systems. We will look at their different aspects regarding e-Voting systems, e.g. the huge number of persons using the biometrics or the small expertise of typical users.

Standard	Gegenstand
ISO/IEC FCD 7816-11	Personal verification through biometric methods
NISTIR 6529 (CBEFF)	Common Biometric Exchange Format Framework www.nist.gov/NISTIR-6529-CBEFF bzw. ~/cbeff [CBEFF is extended by NIST/Biometric Consortium Biometric Interoperability, Performance and Assurance Working Group (www.nist.gov/bcwg)]
XCBF	XML Common Biometric Format: XML-Schem to exchange biometric data via Internet www.oasis-open.org/committees/xcbf/
ANSI B10.8	Finger minutiae extraction and format standard for one-to-one matching
ANSI/NIST ITL 1-2000	Data format for the interchange of fingerprint, facial, and scar mark & tattoo (SMT)
ESIGN-K	EU standard for digital signature cards (PIN and biometric authentication) draft: www.ni.din.de/sixcms/detail.php3?id=389
DIN V64400	Finger minutiae encoding formats and parameters for on-card-matching
BDPP	Biometric Device Protection Profile (UK) www.cesg.gov.uk/technology/biometrics
FBPP	Federal Biometric Protection Profile (US-DoD) http://niap.nist.gov/cc-scheme/PP_BSPP-MR_V0.02.html
BioAPI(ANSI/INCITS 358-2002)	Consortium for standardisation of communication interface between application and biometric devices www.bioapi.com
HA-API	Human Authentication Application Program Interface: US Ministry of defence initiated project. It was merged after version 2.0 in 1998 with the BioAPI-Consortium.
BAPI	Biometric API von I/O Software: Proprietary biometric interface of Microsoft.

Figure 1: Biometric standardisation efforts (Source: heise.de)

One of the main issues we like to stress is the difference between biometric authentication compared to "classic" authentication as e.g. smart cards. In this comparison we ignore the well known concept of card readers based on biometrics, e.g. card readers with fingerprint authentication; In this case, the biometric input is not used to authenticate the user to the e-Voting system, but rather to authenticate his/her smart card. The e-Voting system does not interact in any way with the biometric characteristics of the actual users, but still authenticates the user with the help of the user's authentication certificate as present on the card. Seen from this perspective, this solution is not a biometric approach to e-Voting. From now on, we will focus on biometric approaches that actually use the biometric data to authenticate the e-Voting system. Another issue with biometric systems is their relative young age, there is still currently a set of standardisation efforts going on (see Figure 1).

We will first have a look at some of the possible biometric properties that can be used for the authentication of individual persons. In this paper, we will restrict ourselves to present just a subset of different biometric properties. We explicitly do not focus on their feasibility, but rather try to show the wide spectrum of "theoretically" possible human properties that can be used in biometric systems.

Fingerprint. Fingerprint scanners are probably the most commonly used biometric system; as and replace the pin code entry to unlock the card, especially in the area of smartcard readers. Similar systems include hand geometry or palmprints [html1] [html4].

Iris. Another static property of individuals are eyes. One can either use pictures of the person's iris or use a retina scanner that scans blood vessels to create an individual data set.

Face. The human face is also a feature that can be used by biometric systems. Human face recognition by analysing the size and position of different facial features is being pushed for use at several airports to increase security. Another possible approach is to make infrared recordings and analyse the resulting facial thermogram [html3].

Voice. A more behavioural individual aspect of humans are their voices. Everybody has a special mode and tone while speaking. Voice recognition tries to analyse these features and use them to identify a person [html2].

Signature. Another behavioural aspect of a person usable by biometrical analyses is the signature. Not only the form but also the dynamic aspects can be seen as a set of unique features of a person. Other possible movable biometric input could be the rhythm and pattern of a person's walk.

DNA analysis. Now this is a rather more theoretical idea for biometric identification. Imagine a DNA reader that can create a full DNA analysis within seconds from just a few cells of a person's body. Such a device would surely be a match to, e.g. a finger print reader, when comparing the quality of the results.

Multi-Biometric Systems. As a final approach to biometric data gathering, one can combine two or more actual biometric analyses and combine their results, i.e. use more than one uni-biometric system. This combination yields better results than each of the combined analyses individually and thereby increases the reliability of the biometric system.

With this we tried to give a quick introduction to the different kinds of biometric systems and will now focus on some of their technical aspects which are relevant to an e-Voting system. Initially, we will concentrate on the infrastructure required to use biometric input as the authentication means for an e-Voting system. As already mentioned before, we will not look at localized biometric measures, e.g. fingerprint scanner on the smart card reader that replaces the normal pin code, but focus on the truly biometric input to the actual e-Voting system.

If we look at such e-Voting systems, we need to have some type of central storage that handles the biometric templates of the users. This data storage again imposes high security demands, it must be impossible to tamper with the biometric templates, as this would enable fraud. An attack on the templates can come from two directions:

- A third party could replace a number of biometric templates against other templates which would allow them manipulate the results of the vote.

- Even if the risk of the above attack is seen as neglectable, there is one attacker that has a much more direct access to the biometric templates: the government. This opens a relatively straight forward route to manipulate the votes in a favourable direction for the currently governing party. One may state now that this is already possible – as many examples have unfortunately shown – even if using "old-style" paper votes.

However, the danger of this happening unnoticed is much larger. In a paper based voting scheme, large scale fraud involves a large number of people. Therefore, the risk of an information leak is several degrees higher than in an electronic environment where frauds on a similar scale can be executed in an automated manner by just a few people.

The two attacks mentioned above try to move the result of the vote into a direction favoured by the attacker. However, there is a second type of attack that is rather destructive. In this case, the goal of the attack is not to change the outcome of the vote, but rather to prevent a result of the vote in the first place. Again there are two possibilities for the attacker. Either, he starts the attack before the actual vote starts, or he initiates the attack after the vote has started, e.g. using distributed denial of service (DDOS) attack on the servers with the biometric templates. The second approach has two advantages. First, it gives the service provider of the vote a very limited time to react to the vote. Second, one has to take into account the psychological consequences such an attack has on a person not able to give his/her vote.

After taking a look at a selection of biometric properties, as well as the required infrastructure with its weaknesses, we will now set out a list of criteria that allows us to classify biometric systems.

Cost. The cost factor is very important for e-Voting systems as the number of participants tends to be very high. Each and every participant needs to spend an initial amount of money for his/her biometric reader. Depending on the recorded biometric characteristic, these costs can be rather large.

False Reject Rate (FRR). No biometric system is perfect. One of the problems that can occur are so called false rejects. A false reject is the situation where a valid user tries to authenticate and is falsely rejected by the system (see Figure 2).

One way such a false reject can happen is due to noise in the recorded biometric data, e.g. a fingerprint with a new scar or a voice altered due to a cold. Noise can also be introduced due to altered environmental conditions, e.g. humidity on a capacity finger print reader or unfavourable illumination for a face recogniser. If this "noisy" data is matched with the stored user templates, the difference can be too big and the authentication fails, i.e. the user is rejected.

Another issue with the universal applicability of biometric systems is the possibility that a user is not able to participate, as he/she does not have sufficient biometric properties within the measured domain, e.g. his fingerprints were burnt during a fire.

Final effects that may cause a false reject are time dependent variations either with the individual, e.g. tone of the voice changing over time or an accident that changes the individual's signature, or a variation due to the reader, e.g. a new version of the reader uses slightly different sensors that yield slightly different measurements.

	False Reject Rate	False Accept Rate
Fingerprint[1]	0.20%	0.20%
Voice[2]	10-20%	2-5%
Face[3]	10%	1%

Figure 2: FRR and FAR for three example biometric systems

If a biometric device is used as an access control mechanism, a false reject may be acceptable, as it may only require the user to use a different means of authentication, e.g. by calling security, to access the area from which he was excluded by the authentication system. In the context of e-Voting, a false reject means to deny an individual of the possibility to execute his/her right as a citizen. An e-Voting system using biometrics has to cope with such scenarios.

False Accept Rate (FAR). The second type of error a biometric system is doomed to make is a so called false accept. In contrast to false rejects, a false accept means that a user is successfully accepted (authenticated) even though he/she should have been rejected. In an e-Voting system there are actually two scenarios where we have to talk about false accepts (see Figure 2):

- An unauthorized user is erroneously accepted for a vote. This has two consequences. First, this user is able to give a vote and thereby to possibly change the vote's outcome. Second, as the wrongly authenticated user already gave his vote, the actual user that should be allowed to vote is wrongly rejected yielding the same result as with a false reject.

- An authorized user is confounded with another valid user. With this the short-term effect does not yield a wrong vote count. However, once the other user is trying to make his/her vote, he will be rejected under the assumption that he has already made his/her vote. This again leads to all the consequences of a false reject.

Another source of false accepts is the uniqueness of the tested biometric recordings. Even with assuming that a finger print is actually unique, a finger print reader will not yield different readings for all users. This stems from the fact that a finger print does not yield the complete finger print as a picture for matching against the stored template, but it actually reduces the input to a predefined feature set of typical characteristics. This introduces a theoretical upper boundary on the number of individuals that a biometric system can distinguish between.

Spoofing. Another important aspect of a biometric system is its susceptibility to spoofing. Spoofing is the wilful trail to impose a false accept onto the biometric system. This type of attack is especially relevant for behavioural properties, e.g. replay of a voice recording or a blueprint of a signature. However, face recognition as well as the other physical properties are also susceptible to this type of attack.

As an example we will examine an attack on finger print readers. Modern models do not rely solely on the pattern of the applied finger, but also executes a "Life-Check". [4] describes how members of the CCC try this approach. Their approach is to first get a finger print of the impersonated person using conventional means. This fingerprint is digitally photographed and reworked using graphics software and finally transferred onto a photo layered using acid. This form is then used to make a latex print of the original finger. Due to the very thin layer of latex, it is also possible to trick the "life-check" of the reader.

Costs of the Biometric Infrastructure. In addition to the costs of the biometric readers, the cost of the biometric infrastructure has to be handled. The infrastructure roughly consists of two parts: enrolment infrastructure and voting infrastructure. The enrolment infrastructure is necessary to collect and maintain a database of the biometric templates of all participants. The voting infrastructure handles the actual e-Voting process, i.e. it must be able to handle authentication requests of all participants within the official voting period; Depending on the used biometric mechanism which may require considerable space as well as computing power.

Another aspect of the biometric infrastructure is its high demand on security. It has to maintain the two requirements of a secure e-Voting system: personalisation and privacy. Each and every vote has to be linked to a person while preserving the person's anonymity of what exactly he/she voted for.

Fail Safety of Biometric Infrastructure. In an access control system, a failure of the system may be acceptable. There will be a way to bypass the system and go back to a manual authentication mechanism, e.g. using guards and controlling some form of paper ID. With an e-Voting system, this is not acceptable. Let's assume an ongoing one day vote from 8:00 in the morning to 2:00 in the afternoon. At 9:00, an attacker starts a DDOS attack on the biometric infrastructure that actually blocks it and denies most citizens to actually process their votes. In the best case, it may be sufficient to repeat the vote at a later time. However, in other scenarios, it may have much more serious consequences.

Scenarios, such as the one described with the DDOS attack are quite common nowadays. As e-Voting systems become more common and votes on larger scales are handled by them, the danger of such attacks becomes more and more imminent.

Acceptance of Biometric Infrastructure. The final factor for a biometric user authentication mechanism is its acceptance with its users. Voting is mostly a matter of trust. Regardless of its actual security, a voting system (electronic or not) is only as good as its acceptance with its users. Therefore, any introduction of a new voting system requires a good deal of work to increase its acceptance with the future users. This is especially true with biometric systems [Si02]. Increasing the acceptance of such e-Voting systems is probably a slow process.

5 Conclusions

Disregarding security, e-Voting systems can use biometric user authentication. However: Is this necessary? Is it worth the effort and are the security risks manageable? We cannot give an answer to these questions within the scope of this paper. We also cannot give an answer to these questions that is globally applicable. The main conclusion of this paper is that biometric approaches for e-Voting systems should be extremely carefully deployed. Actually, we would even recommend to refrain from using biometric systems in this context (at least for the moment). Currently, the rejection rates are just too high for an environment as sensitive as electronic votes.

Properties that have to be improved include:

- False accept rate
- False reject rate
- Protection against spoofing attacks
- Judicial aspects regarding access to biometric templates

References

[html1] Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2002/

[html2] The 2000 NIST Speaker Recognition Evaluation, http://www.nist.gov/speech/tests/spk/2000

[html3] Face Recognition Vendor Test, http://www.rfvt.org/FRVT2002

[html4] Latex versus Biometric, http://www.heise.de/ct/03/18/052/default.shtml

[html5] Implementing Electronic Voting in the UK, http://www.odpm.gov.uk/stellent/groups/odpm_localgov/documents/pdf/odpm_locgov_pdf_605188.pdf

[html6] USACM, Policy Brief: E-Voting Technology and Standards, http://www.acm.org/usacm/Issues/EVoting.htm

[html7] NIST Voting Standards Symposium, December 2003, http://realex.nist.gov/votingstandards/

[html8] http://www.swissinfo.org/sde/swissinfo.html?siteSect=2051&sid=1575998

[html9] http://www.revue.ch/de/content/fuenfte_schweiz/e_voting.php?navid_meta=3

[html10] Equal access to electoral procedures, Good practice guidance, http://www.electoralcommission.gov.uk/files/dms/GoodPracticeequalaccess-finalversion_11561-9041__E__N__S__W__.pdf

[Ba04] J. Bannet, D.Price, A.Rudys, J.Singer, D.Wallach, Hack-a-Vote: Security Issues with Electronic Voting Systems, IEEE Security & Privacy Vol2 Nr1 p32

[Br03] Braun, N., P. Heindl, et al. (2003). e-Voting in der Schweiz, Deutschland und Österreich ein Überblick. Arbeitspapiere zum Tätigkeitsfeld Informationsverarbeitung und Informationswirtschaft. Wien, Wirtschaftsuniversität. 2003,2.

[Cr02] Crown, e-Voting Security Study, Issue 1.2, 2002

[Ev04] D. Evens, N. Paul, Election Security: Perception and Reality, IEEE Security & Privacy Vol2 Nr1 p24

[La02] TeleTrust Deutschland, G. Lassman, Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, 2002, http://www.teletrust.de/down/kritkat_2-0.zip

[PKK03] Alexander Prosser, Robert Kofler, Robert Krimmer; Deploying Electronic Democracy for Public Corporations, proc. EGOV 2003, p234-239

[Si02] Richard Sietmann, Im Fadenkreuz: Auf dem Weg in eine andere Gesellschaft, http://www.heise.de/ct/02/05/146/default.shtml

[Sm03] Ella Smith, Ann Macintosh; E-Voting: Powerful Symbol of E-Democracy, proc. EGOV 2003, p240-245

[Zi03] Peter-Michael Ziegler, Europas größte Gesichtserkennungsanlage im Zoo Hannover, http://www.heise.de/ct/03/09/026/default.shtml