e-voting.cc

Competence Center for Electronic Voting and Participation

SECURE REMOTE VOTER REGISTRATION

August 2008

Jordi Puiggali
VP Research & Development
Jordi.Puiggali@scytl.com

scytl Secure Electronic Voting

Index

Voter Registration

- Voter registration is the process to collect the voters' data in order to constitute an electoral roll and/or request an special way of voting (e.g., postal voting)

- The electoral roll determine if a voter has the right to cast a vote during the voting phase, therefore, it has to be formed in an secure way

- A deficient voter registration system can facilitate fraud practices that can affect the accuracy of the election:
  - On April 2008, the report "Purity of Elections in the UK, Causes for Concern" (Stuart Wilks-Heeg, University of Liverpool) highlighted a cases of registration fraud on postal voting in the UK.

Voter Registration Models

- In person
  - Voter requires to attend to a physical place in which his/her identity is verified (e.g., registration office or embassy)
  - Used for updating the electoral roll information and/or requesting absentee voting
- Remote
  - Voters fill in a form with his/her personal details and send it to the register officer through a communication channel
  - E.g., voter fills in a paper form and sends it through postal service
  - Used mainly for requesting absentee voting (e.g., postal voting)

Index

scytl Secure Electronic Voting

Registration process workflow

- Voter fills in a registration form
  - Voter introduce personal and contact details in a form provided by the election officials (e.g., paper registration form)
- Voter delivers the registration form
  - Voter sends registration form to the election official through a delivery channel (e.g., postal service)
  - Voter's usually includes an identity proof with the registration form (e.g., hand writing signature and/or personal details)
- Election authorities verify the received registration form
  - Election officials verify the identity of the voter (using the identity proof attached to the registration form) and his/her right to vote
  - Based on the result of the previous identification process the voter status is updated (e.g., added to the list of absentee voters)

Voter registration channels

There are two common remote voter registration channels:

- Postal (e.g., UK, US…):
  - Registration paper forms are usually available to voters through postal delivery or downloading them from the network.
  - Voters fill out, hand-writing sign and return the forms to the registration officers using a postal delivery or optionally attending in person to a registration site.
- Electronic (e.g., US):
  - Voters fill in an electronic registration form (e.g., webpage) or scans a pre-filled in paper form.
  - The electronic form is send to the election officers using an electronic channel (e.g., the same web page or through a FAX).
  - The identity proof is usually some personal information that is assumed only known by the voter (e.g., birth date) or digitalized hand-writing signature.

Voter authentication

The accurate authentication of voter (i.e., the authenticity proof) is of paramount importance for guaranteeing an accurate electoral roll.

Currently is by one or the combination of the following techniques:

- *Verification of personal information of the voter*.
  - It consist of checking if the voter has included in the form some personal information that it is also stored in the voter register (e.g., birth date, social security number, mother maiden name, etc.). It could be easy to impersonate a voter in the registration process just using this information

- *Verification of some physical characteristics of the voter*.
  - It consists of verifying the identity of the voter based on some voter personal characteristics (i.e., biometrics). On remote registration only hand-writing recognition is usually supported.
  - This is more secure than the previous one

Main security requirements

- Accuracy to validate the voter identity.
  - It depends on the ability of the registration officers to validate the voter identity proof.
- Prevention of multiple registers by voter.
  - Current remote voter registration methods do not check if the same person has filled out more than a registration form by using the names of different valid voters.
- Integrity of voter registration information.
  - The contents of the registration form can be altered or copied after this form has been sent by the voter.
  - This could enable the impersonation of voters by means of replay attacks.

Hand-writing signatures cannot fulfill all this requirements. Any alternatives?

Index

Requirements

The performance of biometric systems is evaluated by the following requirements:

- Universality. Each individual should have the characteristic.
- Uniqueness. It is how well the characteristic makes different two individuals.
- Permanence. It is how well the characteristic endure over the time.
- Collectability. Ease to acquire the characteristic.
- Performance. It refers to the speed and accuracy of recognition as well as the resources required to do it (cost).
- Acceptability. It indicates the level of acceptance of people to use the characteristic.
- Robustness. It reflects the level of resistance against fraudulent methods attempting to mislead the system.

In a remote environment we have voter technology constraints for acquiring biometric information. Best candidates:

- Hand-writing: Acquisition by means of paper forms.
- Voice: Acquisition by means of standard phone.

Requirements (ii)

Taking fingerprint biometrics as reference, the proposed biometrics systems fulfill the requirements previously introduced as follows:

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Robustness
Fingerprint	H	H	H	M	H	M	M
Off-Line signature	M	M	L	H	L	H	L
Voice	M	M	M	H	M	H	L

L=Low
M=Medium
H=High

Off-line signatures and voice biometrics are not as robust as fingerprint biometrics systems. However, the introduction of voice biometrics could improve the current systems based on hand-writing signatures.

Accuracy

- *False rejection rate* (FRR). It is the percentage of valid users declared by the system as non-eligible
- *False acceptance rate* (FAR). It is the percentage of invalid users identified as valid by the system.
- *Equal error rate* (ERR), the point at which FRR and FAR are the same.

Biometrics	FRR	FAR	EER
Fingerprint	2.2%	2.2%	2.2%
Off-Line signature	10-30%	10-30%	10-30%
Voice	5-10%	2-5%	6%

Fingerprint is the best positioned biometric characteristic. However, voice biometrics behaves better than hand-writing signatures.

Preventing Multiple Registration

There are two main operation contexts implemented by biometric systems for user authentication:

- *Verification. T*he system verifies a user identity by using a unique identifier that allows to locate his/her biometric template on the current biometric database.
  - The user gives a personal ID or username known by the system.
  - The system retrieves the template related to the user and carries out a one-to-one comparison.

- *Identification.* Based on the biometric characteristic given by the user, the system has to identify if such characteristic corresponds to one stored in its database. In this case, a one-to-n comparison is carried out.

Current remote hand-writing signature methods only use the verification context.

Using voice biometric system in the identification context, the signature of the register could be checked against the complete database of signatures stored. Then, in case the same voter attempts to register more than once using different personal information, she will be detected.

Integrity of information

- Attaching biometric information to a registration form does not always guarantee the integrity of the form contents, nor prevents reusing this biometric information to impersonate a voter

- A usual method to protect information is the digital signature. However, digital signatures have important logistic problems, for example it is necessary a PKI to generate and provide users with digital certificates

- Only biometric systems that can obtain the voter identity from the registration information could protect the integrity of this information:

    - Hand-writing biometrics as well as voice possesses that peculiar characteristic, which is the binding that can give between the biometric characteristic and the contents of the message.

    - Fingerprints and hand-writing signatures are not obtained from the registration information, only from the identity proof

Index

Objective: propose a remote electronic registration method more robust than current one

Four participants are necessary during the voter registration process:

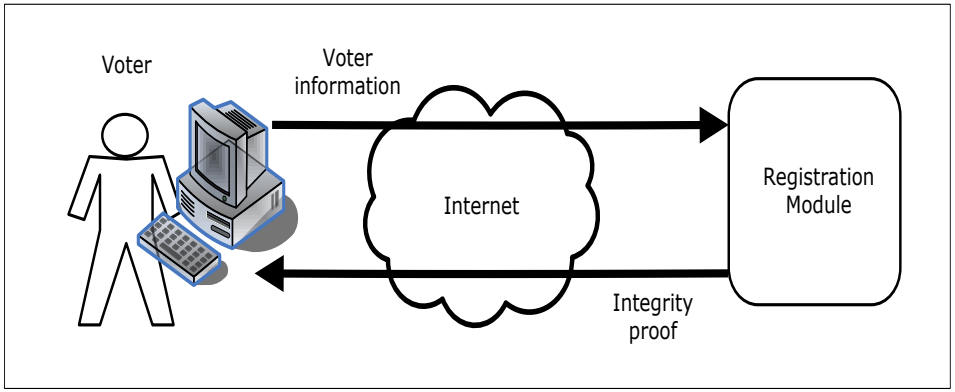
- *Voter.* The voter provides her personal data in order to generate the registration information.
- *Registration module*. This module is used to enter the voter registration information and generate an integrity proof.
- *Validation module*. The registration proof is generated by means of this module. Such proof is generated with the biometric information provided by the voter.
- *Registration officers*. The registration officers receive the voter register information and carry out some validation processes.

The process is divided in two main stages:

1. Voter registration information gathering and integrity protection
2. Generation and validation of a registration proof

Voter registration information gathering and protection

- The voter connects to the Web site of the Registration Module by means of a secure and encrypted channel, e.g. SSL.
- The Web site provides a registration form.
- The voter fills in the registration form with his or her required personal data.
- Once completed the registration form, an integrity proof is generated by the Registration Module. Such integrity proof is a cryptographic hash function of the registration information provided by the voter.
- The integrity proof is then represented in a format that can be read by the voter, for instance, a base-32 notation. This representation is shown to the voter by means of the same communication channel.



Details of the integrity proof

Generation of the integrity proof

1. Get a digest *k* from the registration information

$$Mi : K = \text{MD5}\ [Mi]$$

2. Use *k* as a key to get a HMAC-SHA1 from the same registration information *Mi* :

$$H = \text{HMAC-SHA1}\ [Mi, K]$$

The resultant *H* is the integrity proof.

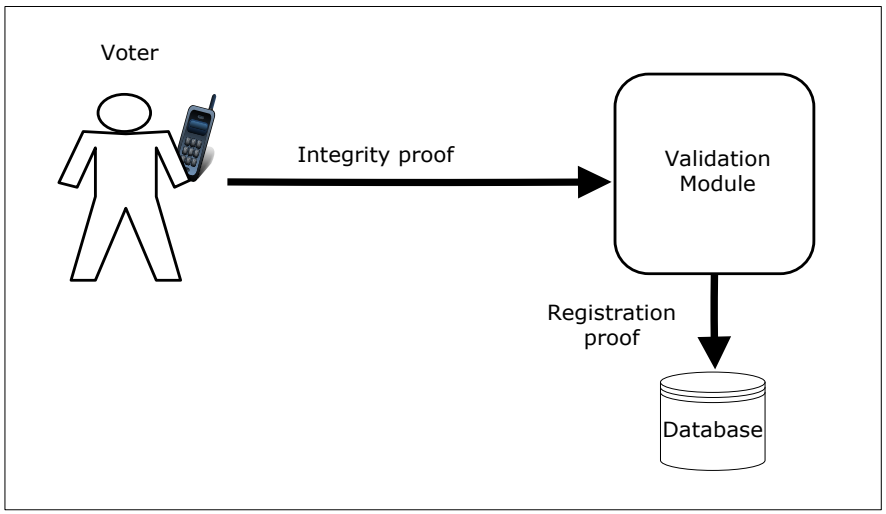
- Using a combination of MD5 and HMAC-SHA1, the probability to have a collision decreases significantly. An attacker needs to find a coincidence of collision for the same text on both systems. In addition, we are reducing the probability of these collisions without increasing the size of the digest that remains the same as a SHA1 (160 bits).

scytl Secure Electronic Voting

Generation of the registration proof

Based on the previous analysis, we will use a voice biometric system in this stage.

- The voter carries out a communication with the Validation Module by means of a phone call.
- The voter is asked to give the integrity proof. Then, he or she speeches the proof previously shown by the Registration Module, i.e. the groups of characters that represent the integrity proof.
- The voice of the voter is bound to the contents of the registration information. This is called the registration proof.
- The registration proof is stored by the Validation Module.



Details of the registration proof

- The registration proof protects the integrity and provides authenticity of the registration information.

- The interaction between the voter and the Validation Module includes, besides the speech of the integrity proof, other dynamic data in order to prevent reply attacks in which an attacker could use a pre-recorded voice of a voter. Such dynamic data could consist of a challenge to the voter who has to repeat a word or a set of words said by the Validation Module. That way, the Validation Module can be sure that the integrity proof is being speech by a person who is on the other side of the communication line and not by a pre-recorded or automatic process.

- Once the registration officers have recorded the validation proof, they can start the validation process.

scytl Secure Electronic Voting

Validation of the registration proof

- The validation process facilitates the detection of people who attempts to create more than one record. It is possible to compare the voice of a voter who is validating a new registration with the set of voices previously recorded. This verification is not necessarily carried out on-line.
- The scheme does not require a previous database with the recorded voice of voters. However, for future registrations, the previous records can be used in order to validate the voice of the voter who is making the new record.
- An additional validation consists on checking the voter registration information against the associated registration proof. This check will consist on verifying if the integrity proofs match.
- If any of the validations fails, the voter registration form and corresponding registration proof can be classified as non-validated records. Therefore, registration officers can implement addition manual checks or contact the voter for checking the process if required.
- In a subsequent voting stage, it could be possible to use the registration proof to verify that the person who is voting is the same who created the registration information by checking his or her voice.

scytl
Secure Electronic Voting

Index

Conclusions

- Current remote voter registration systems have important issues that can facilitate voter impersonation. These issues are mainly voter identification accuracy, multiple registrations from the same person and voter registration information integrity.

- The use of biometrics systems increases the voter identification accuracy of voters that make a remote registration.

- Operating on an identification context, biometrics systems can automate the detection of multi registrations made by the same person.

- Voice biometrics can bind the registration information to the voter identity. Combining this feature with the use of cryptographic algorithms, such as hash functions, provides a way to protect the integrity of voter registration information that can be suitable to implement in current environments.

www.scytl.com