BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LX No. 2/2008	93-97	Seria Matematică - Informatică - Fizică

e-Voting Security

Ciprian Stănică-Ezeanu

ASE Bucureşti, Informatics Security Master, P-ţa Romană nr.6, sector 1, Bucureşti, 010374
e-mail : cystanica@yahoo.com

Abstract

The aim of this paper is to present e-voting procedure describing its advantages and disadvantages. Conventional security measures such as firewalls or SSL communications are necessary but not sufficient to guarantee the specific security requirements of e-voting. Besides these conventional security measures, it is also necessary to implement an additional layer of specialized security technology to address the specific risks posed by electronic voting and guarantee critical security requirements such as voters' privacy, vote integrity and voter-verifiability.

Key words: *e-voting, security, vulnerability*

Introduction

In an attempt to modernize our election process by moving from paper ballots towards the world of digital computers, governments might be jeopardizing our democracy. Many politicians and legislators are in favor of electronic voting. They see a lot of possibilities in this new technology. Most proponents argue that the adoption of e-voting systems would increase voter participation. Increasing voter participation is of interest because voter turnout has been low and declining in most countries. Election directors are also quick to pick up on the argument that electronic voting may be the cheapest, quickest and most efficient way to administer elections and count votes. However, the cost of online voting would vary enormously depending on the type of system employed and the type of security used. But from the first trials with e-voting, there has been a lot of concern about the security of computer-based voting systems. Online voting systems have a lot of technical vulnerabilities.

e-Voting Concept

Besides a German set of - governmentally commissioned - requirements for on-line election systems expected in the first half of 2004, the Geneva "11 commandments for internet voting" are of special interest as they incorporate experiences with E-voting [1]:

1. Votes cannot be intercepted nor modified;
2. Votes cannot be known before the official ballot reading;
3. Only registered voters will be able to vote;
4. Each voter will have one and only one vote;
5. Vote secrecy is guaranteed; it never will be possible to link a voter to his/her vote;
6. The voting website will resist any denial of service attack;

7. The voter will be protected against identity theft;
8. The number of cast votes will be equal to the number of received ballots;
9. It will be possible to prove that a given citizen has voted;
10. The system will not accept votes outside the ballot opening period;
11. The system will be audible.

In order to introduce this type of voting it is better to accept some ideas as following:

- suggest e-voting as additional, optional voting channel;
- start with identifiable group(s) of persons who wish / need e-voting, e.g. persons away from polling stations on election day(s), handicapped and bedridden persons incapable of going to polling stations, and mobile and busy people unwilling to go to polling stations but interested in participating in elections;
- go for added-value schemes which may be different in individual countries, with respect to existing voting channels and procedures;
- full understanding and trust by voters and lawmakers - including of the opposition - are absolutely necessary;
- only a step-by-step approach leads to success: election tests separate from or parallel to, elections are to be held before valid test elections (pilots) can be, and small before big numbers of electors should be involved; - in countries where postal voting is practiced, extending postal voting to remote e-voting eases the introduction of e-voting;
- the best, as most reliable way, is identification with the help of electronic signatures / smart cards (not PINS);
- in order to avoid risks through postal transmissions, any transmission related to e-voting shall be possible / offered by electronic channels.

Public confidence in the election process depends on the verifiability of an election. There must be assurance that all votes cast are indeed counted and attributed correctly. As each vote is cast, an unalterable record must be created ensuring a verifiable audit trial. Electronic voting is likely to lead to changes in how the public maintains confidence in the integrity of elections. With e-voting systems, public confidence in the election relies on trust in technical experts instead of a transparent process. Media stories about security threats to the Internet have an immediate impact on public confidence and past failures have made people distrustful. Electronic voting may not achieve the goal of increasing turnout if voters do not trust it. There are many ways to make electronic voting more secure. Mechanisms that form the structure of security are for instance Personal Identification Numbers or passwords, encryption, digital signature, smart cards or biometric identifiers.

Voter-verified Audit Trial

A voting system is only as good as the public believes it to be. A way to provide a voter-verified audit trial (VVAT) was proposed by Rebecca Mercuri [2]. Her method requires that "the voting system prints a paper ballot containing the selections made on the computer. This ballot is then examined for correctness by the voter through a glass or screen, and deposited mechanically into a ballot box, eliminating the chance of accidental removal from the premises. If, for some reason, the paper does not match the intended choices on the computer, a poll worker can be shown the problem, the ballot can be voided, and another opportunity to vote provided.

Once the voter has cast his ballot and left the polling booth, no one will be able to detect or correct possible errors that the machine made in recording the votes. Computer scientists say that the solution is relatively simple; all voting equipment should require a VVAT which provides a permanent record of each vote. This way the voter can check to ensure that it represents their intent. It is vital that the voter doesn't keep the paper so that he can't prove to someone that he has voted a certain way and get paid for it. When there is any doubt about the results of the election, there is the possibility of a manual recount.

A reason why more scientists started to worry about electronic voting systems without VVAT was the uproar about the Diebold voting system. Numerous reports have found Diebold machines and other computer voting systems vulnerable to error and tampering [3].

Election security must be viewed as a combination of numerous layers of security that, taken individually may be insufficient, but taken as a whole, provide accurate, secure and accessible elections.

If citizens see e-voting as a convenient way to cast their votes, they might be less concerned about its security issues. This could also work the other way around. A system could be one hundred percent safe and secure, but if users don't trust it they will not use it.

Biometric Identification in e-Voting

One of the main issues which is liked to stress is the difference between biometric authentication compared to "classic" authentication as e.g. smart cards. In this comparison it's ignored 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, I 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 standardization efforts going on.

Some of the possible biometric properties that can be used for the authentication of individual persons are:

a. 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 palm prints.

b. 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.

c. Face. The human face is also a feature that can be used by biometric systems. Human face recognition by analyzing 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.

d. Voice. A more behavioral 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.

e. Signature. Another behavioral 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.

f. 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.

g. 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.

Looking at such e-Voting systems, they 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 favorable 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 favored 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.

Analysing the security of e-voting systems it was observed a series of vulnerabilities to the fraudulent attacks. The IT experts from Brennan Centre gave six recommendations for an acceptable e-voting security [5]:

1. Systematic control of identity

Comments: It is necessary a special software for the voter authentication (using biometric methods or smartcards)

2. Random controls in pool-sites

Comments: It must be made each election day in order to discover instantly the attacks of Direct Recording Electronic voting terminals.

3. Interdiction of wireless systems

Comments: They are very vulnerable at attacks.

4. Adoption of an unique system of audit proceedings

Comments: Increasing the reliability of auditing systems in order to assure a higher efficiency.

5. Decentralization of voting systems to the jurisdictional level

Comments : It is more difficult to organise simultaneously an attack in different geographical locations.

6. Adoption a recovery procedure for bugs and attacks

Comments: Finding solutions for all observed system problems.

Conclusion

As broadly accepted, electronic voting and electronic consultation have the potential to improve our electoral processes and enhance democracy in many ways. However, electronic voting is not problem-free. A whole new set of risks and challenges is created by this new voting scenario that is based on the use of electronic voting systems. These risks and challenges can be broadly classified in three categories: legislative, socio-political and technological. Each category have a great importance for a correct election procedure, but only the technological part is our duty.

References

1. Buchsbaum, T.M. - *Proceedings of Electronic Voting in Europe Workshop*, Schlos Hofen (Austria), 2004
1. * * * - http://prodman.wu-wien.ac.at
2. Feldman, A.J., Halderman, J.A., Felten, E.W. - USENIX/*Accurate Electronic Voting Technology Workshop* (EVT'07), Boston, USA, 2007
3. Hof, S. - *Proceedings of Electronic Voting in Europe Workshop*, Schlos Hofen (Austria), 2004
4. * * * - http://www.journaldunet.com/solutions

Securitate în e-Voting

Rezumat

Scopul acestei lucrări este de a prezenta procedura de e-voting, descriindu-se avantajele şi dezavantajele ei. Măsuri de securitate convenţionale precum Firewalls sau comunicaţiile SSL sunt necesare dar nu suficiente să garanteze cerinţele specifice de securitate ale e-voting-ului. În afara acestor măsuri convenţionale de securitate este de asemenea necesar să se implementeze un nivel adiţional de tehnologie de securitate specializată pentru riscurile pe care le implică votarea electronică şi să garanteze cerinţele de securitate critice, precum confidenţialitatea votanţilor, integritatea votului şi verificabilitatea acestuia.