Electronic Voting

An introduction and review of technology

Lawrence J. Brachfeld

University of Colorado at Colorado Springs

Colorado Springs, CO.

*Abstract*—Electronic Voting (E-voting) system is a voting system in which the election data is recorded, stored, and processed primarily as digital information. E-voting offers the potential to be the most reliable, secure, and trustworthy form of voting ever implemented. The underlying digital technology with error correction, robust storage, cryptographic security, and biometric technology provides opportunities to record, transmit, store, and tabulate votes far more reliably than the current voting systems.

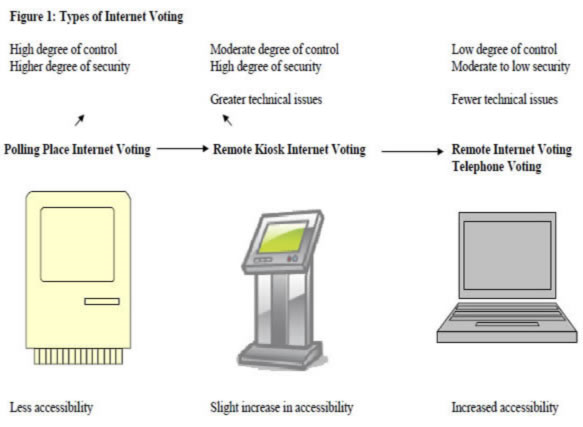
Keywords- Electronic Voting, Biometrics, PKI

# Introduction

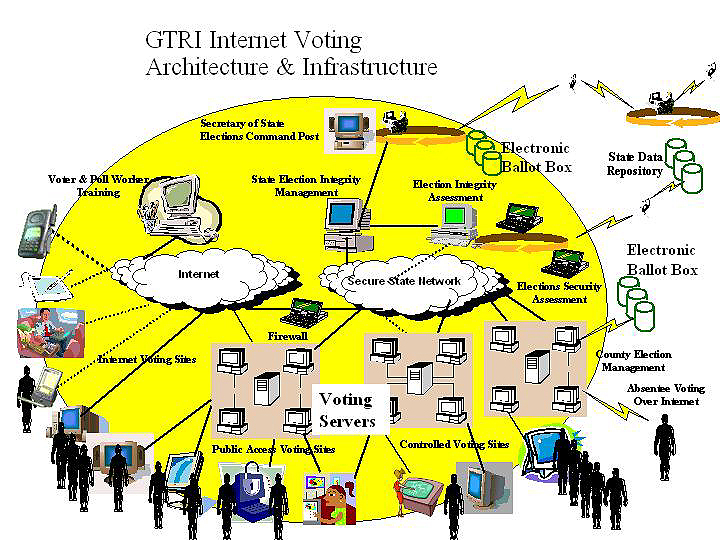
Prior to delving into the discussion of Electronic Voting (E-voting) I intend to clarify my use of several terms:

1. Polling Place Internet Voting – Voting is done at any valid polling place by using a computer under the physical control of election officials to cast a ballot over the Internet [1].
2. Remote Kiosk Internet Voting – Voting is done at your personally designated polling location by using a computer under the physical control of election officials to cast a ballot over the Internet [1].
3. Remote Internet Voting - Voting by using a computer that is not under the physical control of election officials and the ballot is cast over any Internet connection (Dial-up/Telephone or other) [1].

These terms are depicted in Figure 1 below:



Proponents of E-voting make several arguments in its favor. First, E-voting makes it easier for voters to participate in an election because every computer that has an online connection becomes a potential polling site. Second, E-voting may also lower the cost of voting for the entire electorate. Third, E-voting has the potential to eliminate many of the factors that voters use as excuses for not voting, such as weather, long lines, etc. With E-voting, voters can vote from the comfort of their home, public library, or local Internet hot spot. Fourth, E-voting could even allow voters with disabilities much easier access to polls. In December 2001, the Georgia Tech Research Institute (GTRI) began to study the social and technical issues related to E-voting. The architecture and infrastructure diagram they used begins to show how complicated this may be [2]. One of the largest hopes of supporters of E-Voting is that it will tap into one of the largest and most difficult to reach groups of voters, those between the ages of 18 and 25. These young Americans are typically well-versed in using the Internet and may potentially be more comfortable using this technology.



# E-Voting Issues to be addressed

There are several key issues that any E-voting system must successfully tackle in order for the voters to be assured that the system is reliable. I will discuss those here and then delve into the general functional requirements and then the more specific security requirements for E-voting systems.

## Voter Authentication

This involves the process for determining that a ballot arriving at the vote server really is from the registered voter it purports to be from.

## Ballot Privacy

This involves preserving the secrecy of the ballot so that no unauthorized person can read the ballot and more importantly, no one can associate a ballot with the person who cast it.

## Ballot Integrity

The point of this is to provide an extremely high level of assurance that ballots cannot be surreptitiously changed by any software agent or third party.

## Reliable Vote Transport and Storage

This involves guaranteeing that no ballot is either created, lost, or destroyed anywhere from the vote client to the vote server without detection, and no ballots at all are created, lost, or destroyed at all from the vote servers to the vote canvass computers.

## Prevention of Multiple Voting

This involves insuring that no more than one ballot may be counted for any single voter.

## Defense Against Attacks on the Client

This involves guaranteeing that there is no malicious software (Trojan horse, virus, etc.) on the client that can affect the integrity or privacy of the ballot.

## Defense Against Denial of Service Attacks on the Vote Servers

This involves methods for handling deliberate attacks intended to control, crash, or overload the vote servers or the networks they are attached to. These methods may include firewalls, Intrusion Detection Systems, etc.

# E-Voting functional (general) requirements to be addressed

The functional requirements of an E-voting system specify, in a well structured way, the minimum set of services that the system is expected to support:

1. Provide the entire set of required services for organizing and conducting a voting process.
2. Support, in accordance with a well-defined operational framework, all users that have a need to interact with the system.
3. Support different types of voting processes, such as organizational elections, primary elections, and general elections.
4. Be customizable with respect to the geographical coverage of the voting process, the number of voting precincts, the number of voters, and other specific characteristics of the voting process, like start and stop time, number of candidates, etc.
5. Ensure the following:
   1. Only eligible voters can cast a ballot.
   2. No person can vote more than once.
   3. The vote is secret.
   4. Each vote is counted in the final tally.
   5. The voters have confidence that their vote is counted [3].

# E-Voting security requirements to be addressed

The vast majority of security requirements is common to all E-voting systems and is, to a large extent, fulfilled by the voting protocol adopted by the system architecture such as the following:

## Accuracy

Accuracy, sometimes referred to as correctness, demands that the announced tally exactly matches the actual outcome of the election. This means that no one can change anyone else’s vote, (inalterability), all valid votes are included in the final tally (completeness), and no valid vote is included in the final tally (soundness) [3].

## Democracy

A system is considered to be democratic if only eligible voters are allowed to vote (eligibility) and if each eligible voter can only cast a single vote (unreusabiltiy). Additionally, the system must insure that legitimate votes cannot be altered, duplicated, or removed without being detected.

## Privacy

No one should be able to link a voter’s identity to an individual’s vote, after the latter has been cast (unlinkability). There are two types of privacy that we must consider:

1. Computational Privacy – a weak form of privacy ensuring that the relation between ballots and voters will remain secret for a large amount of time.
2. Information-theoretic Privacy – a stronger, but harder to obtain from of privacy, ensuring that no ballot can be linked to a specific voter as long as information theory principles remain sound.

## Robustness

This guarantees that no reasonably sized coalition of voters or authorities, either benign or malicious, may disrupt the election. This includes allowing the abstention of registered voters as well as preventing misbehavior of voters and authorities from invalidating the election result by claiming that any portion of the system failed to properly execute its part. Robustness implies that security should also be provided against external threats and attacks such as a denial of service attack.

## Verifiability

Verifiability implies that there are mechanisms for auditing the election in order to verify that it has been properly conducted. This verifiability can come in three forms:

1. Universal Verifiability – anyone can verify the election outcome after the announcement of the final tally.
2. Individual Verifiability with Open Objection – allows every authorized voter to verify that their vote has been properly taken into account, and to file a complaint, in case the vote has been miscounted, without revealing its contents.
3. Individual Verifiability – allows for individual voter verification, but forces voters to reveal their ballots in order to file a complaint.

## Zero-proof (Uncoercibility)

No voter should be able to prove to anybody else how they voted even if they want to. Additionally, it means that no party should be able to coerce a voter into revealing how they voted.

## Fairness

This ensures that no one can learn the outcome of the election prior to the election official’s announcement of the election result.

## Verifiable Participation

Sometimes referred to as declarability allows the possibility to find out whether a particular voter actually has participated in the election by casting a ballot or not. This requirement is necessary in cases where voter participation is compulsory by law or where abstention is considered to be an extremely contemptuous behavior.

# Authentication techniques

Every remote electronic voting system needs to implement voter identification and authentication techniques to ensure that only eligible voters may cast a vote and those who do can only vote once. In information security, mainly two ways of identification and authentication are known (as well as corresponding mixed

ones): something you know and something you are. Both techniques are discussed in the following paragraphs with respect to their applicability for E-voting.

## Something You Know: a Secret

The first category is based on knowledge, while two different implementations are possible:

1. The first possible implementation of voter identification and authentication is applied in accordance with the set up of a secure e-mail account: in the election setup phase, it is possible to set up a secure certificate, such as using PKI technology.

Although, easy from the voter’s perspective, it has three weak points:

a. it cannot be excluded, that other persons, who are not authorized for this particular election, set up an account.

b. voters might choose weak passwords or PKI certificate which can be hacked by an intruder.

c. vote buying cannot be excluded, because voters could easily send their login data to a potential buyer.

*2.* A further type of identification and authentication through knowledge of a secret is called voter PIN procedure. The voter PIN, a voter unique code of letters and digits, which is sent by mail to eligible voters in the election setup phase. This variation is rather similar to the above one with respect to the usability issues. However, the costs increase since the eligible voters get their PIN by mail. However, the security increases because only eligible voters have a PIN and this can be generated through the responsible election authority. However, the risk that the PIN will be intercepted by an intruder still exists.

*B. Something You Are: Biometrics*

The second category is based on distinct personal attributes such as fingerprints, retinal scans, voice recognition, facial recognition, etc. The main advantage of biometric authentication is that attributes cannot be forwarded to another person, for instance, vote buyers. Unfortunately, the matching of scanned and stored data does not work perfectly: the system can falsely reject an authorized subject, or it can falsely accept an unauthorized subject. Therefore, each system has a False Rejection Rate (FRR) and a False Acceptance Rate (FAR). In the past, the FRR has been disregarded as FAR is much more important for privacy and integrity issues. In elections, availability is (because of the universal requirement) as important as other properties. From a cost and user-friendliness point of view it makes a difference whether systems are already deployed or need to be introduced for the election. However, the use of PKI & Biometrics is an area that can mitigate the security specific requirements in E-voting and could potentially allow wide scale adoption of E-voting technology.

1. PKI use in an election with the addition of a biometric factor provides much more confidence that the vote you cast is in fact yours and has not been altered, also called non-repudiation.
2. Using a combination of both PKI and Biometrics to encrypt the vote will help ensure that nobody can read your vote, and there will be significantly improved assurances that the vote you cast is in fact yours.

A number of factors have led to the unprecedented growth of biometrics. Chief among them are decreasing hardware costs, growth in networking and e-commerce, and greater emphasis on security and access control. The terrorist act of September 11 has been another major factor spurring innovation in biometric applications. In fact Biometric authentication offers tremendous advantages over competing methods for authentication in the networked world in which we live. Imagine being able to access different resources and assets that we currently access through passwords without remembering a single password. Biometric authentication systems make this possible. Not only do we not have to

remember passwords, with biometrics there is no need even to worry about the password being stolen. A biometric system also offers more security since a biometric attribute cannot be shared - unlike a password, which can be intentionally divulged to others to provide unauthorized access. The use

of a smart card is another popular method for authentication. However, a smart card can be stolen or misplaced - problems that are not present with a biometric based verification system. These advantages, coupled with low costs for capturing and processing biometric information, are leading to the very real potential for biometric options in the E-voting arena. There are still significant social and technological issues to be resolved, but there is progress being made every day.

# Conclusions

## Historically, in non-electronic elections, most verifiability checks were delegated to precinct election officials at each precinct. In E-voting, one of the critical factors to be resolved is to balance the required level of security verses system complexity, balanced with ease of usability. PKI and Biometric technology provides many exciting possibilites to bring efficiencies to the electoral process, which can in turn engender confidence in E-voting processes among the general population, but this technology also brings the possibilities of pitfalls that can best be avoided if systematic, robust decision making processes are used to design and implement solutions appropriate to the election system that the technological system is inteded to benefit.

##### References

1. R. Michael Alvarez and Thad E. Hall, *Point, Click, and Vote: the future of Internet elections.* Washington, DC: The Brookings Institution, 2004
2. <http://gtresearchnews.gatech.edu/newsrelease/VOTING.html>, accessed on 12/3/10
3. Paul S. Hernson…[et al.], *Voting technology: the not-so-simple act of casting a ballot.* Washington, DC: The Brookings Institution, 2008
4. Steven Furnell, Sokratis Katsikas, Javier Lopez, and Ahmed Patel, Securing Infomration and Communications Systems: Princilpes, Technologies, and Applications. Norwood, MA: Artech House, 2008