6.857 Computer and Network Security	Thursday, September 13, 2001

Lecture Notes 3 : Electronic and Internet Voting

Lecturer: Ron Rivest *Scribe: M. Shi, K./J./E. Huang*

The following notes are meant to be read along with the presentation slides. They do not repeat the information in the slides, but instead add relevant comments.

Requirements for Electronic and Internet Voting Systems in Public Elections

David Jefferson is the chairman of a California task force on Internet voting.

1. Voter Authentication

   Voter authentication is important for assuring the validity of an election. In the US today, some places do a poor job of authenticating voters. In North Dakota, there is very little in the way of authentication. If a person can physically get to a polling site, then he or she can vote. In other cases, legal requirements make the logistics of voter authentication very hard. One interesting question is what to do if a person arrives at a polling site, but cannot be authenticated as having a right to vote. One idea is the provisional ballot. The person is allowed to place his or her vote in a sealed envelope, with his or her information written on the outside. If he or she is later authenticated, then the vote will be taken out of the envelope and counted.

2. Delivering the Right Ballot to the Voter

   In Los Angeles, the ballot is printed in 14 different languages, and it is difficult to keep track of who should receive which ballot. Other places require the candidates' names to be rotated, so that the same candidate is not always the first name on the ballot.

3. Accurate Capture of Voter Intent

   A common thread that runs through all these requirements is that the user interface must be superb. A bad user interface can lead to many mistakes by the voters, preventing accurate capture of voter intent. Also note that many voting systems today, such as paper ballots, have the fault that they do not prevent overvotes.

4. Privacy

   The main reason to break the association between a voter and his or her vote is to prevent people from buying/selling votes, as well as to prevent coercion as a method for getting votes. In Internet voting, cryptography will play an important role in keeping information private. Within the information marked as "less private," there are some gray areas that are open to discussion. For example, if the information about who votes and who does not vote is made public, then people could pay others not to vote. A similar problem arises if ballot images are published, because people can use write-in fields to mark their own ballots.

5. General Security Requirements

   One additional requirement is that there must be very few secrets in the system. Most of the system, including all the code, should not need to be secret in order for the system to be secure.

6. Potential Adversaries

   Voters may want to sell their votes. This is the most difficult adversary to defeat. For example, in the US today, a voter using an absentee ballot can sell his or her vote to someone who is able to verify that he or she did vote a certain way.

7. Tools Available to Adversaries

   In general, an Internet voting system should be designed under the assumption that all software code and hardware configurations will be known to adversaries. A distinction has to be made between public knowledge and cryptographic keys, which are private, unless the adversary is an insider. It is hard to make a large complex system work right. Consequently, complex systems are likely to have many security holes exploitable by adversaries. Hence, a voting system must be kept as simple as possible.

8. Software Certification and Authentication

   If a voting system is not simple, there is little chance of being able to verify correctness, robustness, and security. Qualified teams of engineers who were not involved in the design and implementation of the system need to be brought in to examine the software and hardware for possible flaws.

9. Auditability / Verifiability

   That a system needs to be secure and that a system needs to be perceived as being secure are two different requirements. Meeting the first goal does not mean the second goal is satisfied as well. Professor Rivest may be completely sure of the security of a system he designed, but at the same time be completely unable to convince his mother to accept the security of his system.
   The issue of verifiability is a particularly difficult problem, because of the requirement for privacy. The goal is to have universal verifiability: more openness and more transparency, up to the point of almost violating the voter's privacy.

10. Special Hazards of Remote Internet Voting

    One hazard is an Internet link to a fake voting Web site. The person following the link believes he or she is voting, when in reality his or her "vote" is simply being tossed away by the fake Web site. In other words, in Internet voting, the requirement for authentication works in both directions. Not only does the voter have to be authenticated by the server, but the voter needs to know that he or she is communicating with a true voting server.

Electronic Voting

1. Voting Technologies

   The plus side of paper ballots is that a voter knows the archival record of his or her vote when the ballot is created. Also, paper ballots last a long time but for extreme conditions (e.g., fire). Lever machines undesirably leave no audit trails and thus do not allow votes to be recounted. They also do not allow for rotation of candidates on ballots. The MIT political science department has a lever machine, if any student wants to see one.
   Many electronic voting systems today rely on touch screen technology.

2. Error Rates by Technology

   Lever Machines achieve low error rates due to their simple user interfaces.
   The high error rates of electronic voting systems are attributed to both voters' lack of familiarity with the systems and bad user interfaces. With more research on user interfaces, electronic systems have the potential to achieve very low error rates.

3. Electronic Voting

   Election Day should be a national holiday to increase voter turnout and to make voting more convenient. Other measures that achieve voter convenience should not be used if they jeopardize privacy or other requirements. Also, it has not been clearly shown that increasing voter convenience significantly increases voter turnout.

4. Security Requirements

   It is difficult to stop vote buying. Not giving receipts for votes may result in decreased vote buying, but vote buyers can still use tactics such as administering lie detector tests to verify a bought vote. Even without vote verification, just taking a voter's word that he or she will vote for a certain candidate and paying him or her is effective, since it has been shown that people actually do what they say. Also, paying people not to vote can also be very effective.

5. Three Main Categories of Electronic Voting Systems

   - Blind Signatures (e.g., the FOO Voting Scheme) — This is a remote electronic voting system whose key elements are blind signatures of ballots and an anonymous channel for transmitting ballots to be counted. The voter casts a ballot on a remote machine. The ballot is encrypted and blinded, then sent to an administrator who authenticates the voter and signs the blinded ballot. After the ballot is returned to the voter by the administrator, it is decrypted in such a way (due to the magic of blind signatures) that the signature is still valid for the decrypted ballot. The unblinded ballot is then forwarded through an anonymizer to the counter. The anonymizer removes the association between a voter and his/her ballot. Finally, the counter decrypts and counts the votes on the ballot. Even with collaboration by the administrator and counter, they still cannot determine which ballot was cast by which voter. Also, the counter cannot begin counting votes until the election is over. This is to prevent any partial vote counts. FOO and other remote voting schemes do not prevent vote buying. This system supports write-in votes. There is another layer of encryption (called a "commitment" in the FOO paper) that is removed once the election is over.

- Mix-Net — The system encrypts all input ballots and then scrambles/permutes and re-encrypts them to produce anonymized output ballots for counting. A mix-net is a natural way to implement the anonymizer of the FOO voting scheme. This system supports write-in votes.
- Homomorphic Encryption — In this system, individual ballots are encrypted and sent to the counter. The counter uses a mathematical operation to combine the encrypted ballots such that the output of this operation is a count of the ballots in encrypted form. This final count is decrypted and recorded. In this way, individual unencrypted ballots never have to be seen by the counter. This system does not support write-in votes.

6. Some Personal Opinions

   Physical ballots do not necessarily provide better audit trails than electronic systems. Electronic ballots are replicable and can handle digital signatures. However, voters using electronic systems have to trust a mechanism between themselves and the ballot to accurately record their ballot, whereas paper ballots are their own archival records.