Overview of Electronic Voting Methods and Challenges (June 2015)

Kenneth E. Hogue

Abstract—Voting is the primary method by which the populace can tell the governors their opinions on the government. Advances in computing and networking have opened the attractive possibility of Electronic Voting (EV), and governments worldwide have adopted multiple methods to accomplish this. These technologies need to be examined properly to ensure proper handling of votes.

I. INTRODUCTION

Voting is the cornerstone of the majority of societies today, and fair elections are a requirement for a government to be considered legitimate. This task, however, can consume significant time and money to accomplish using paper-based technologies.

With the advent of modern computing and networking capability, two possibilities have emerged to leverage the technology for voting purposes: (1) to deploy electronic voting booths to voting stations for use by the public and (2) to enable voters to use any computer with a network connection to cast a vote. Both of these approaches have challenges that must be adequately addressed to ensure the voting process is fair and transparent.

II. THE RISE OF E-VOTING

Individual voting was devised in a time when hundreds, or perhaps thousands, might participate. At that time, the tools and techniques were simple and the process easily verifiable. As humans developed societies spanning continents and hundreds of millions of citizens, the process of voting became exponentially more complex. The adoption of electronic voting to increase time and accuracy while decreasing cost was an inevitability.

A. The Voting Process In General

The voting process has existed in some form since the ancient times of Greek democracy. Any voting process must include the following features in order to be considered valid [1]:

1. Accuracy: (1) a vote cannot be altered, (2) a vote cannot be eliminated from the count, and (3) an invalid vote cannot be counted.
2. Democracy: (2) only eligible voters can vote one time.
3. Privacy: (1) no entity can identify how a voter voted and (2) no voter can prove how they voted.
4. Verifiability: You can independently verify that all votes have been counted.
5. Availability: (1) the system works properly during poll hours and (2) all voters have access to the system during poll hours.
6. Ability to resume: the system allows any voter to resume the voting process during poll hours if the process is interrupted.

![Fig. 1. The three electronic voting systems currently in use.](image_url)

Fig. 1. The three electronic voting systems currently in use. The top process shows optical scan voting, in which the voter makes a mark on a punch card which is read into a tabulating computer. The middle process direct recording electronic system, which records a vote directly on a computer and transfers it to a central vote-counting server. The bottom process shows electronic home voting, which allows a voter to vote from any Internet-enabled computer and stores the vote in a secure server.

B. A History of Mechanically-Assisted Voting

In 1889, Herman Hollerith submitted a patent application for a punched-card system that could be used to dramatically decrease the tabulation time of census records for the 1890 U.S. Census [2]. The potential for this technology was quickly realized and vote tabulation machines were in use across the country by 1930 [3].

As reliable electronics were developed, vacuum tube and solid state technologies eventually replaced the mechanical systems and more innovations were implemented for use in general elections.
III. ELECTRONIC VOTING MACHINES

The two main variations of electronic voting machines currently used are the Optical Scan (OS) machines and Direct Recording Electronic (DRE) machines. Each system has unique advantages and disadvantages.

A. OS Machines

OS voting consists of a voter marking a physical ballot which is scanned and counted by computer means. The ballots are stored for auditing and for the possibility of a recount. This type of machine is the most common type seen in general use in U.S. elections. The first successful OS machine appeared in 1965 [4].

The first main security concern is one of the oldest in voting: invalid votes being counted in the election, or “ballot stuffing”. The best-practice method to minimize this risk is to keep controls on the printing of the official ballots and to ensure voting personnel follow procedure (i.e., only accept one ballot from one voter). Then, secure storage of the ballots until tabulation is key to address the basic concern of accuracy.

The second main security concern is that of tampering with the vote tabulation machine, which can also affect the accuracy of the vote. As manufacturers adopt the use of commercial PCs instead of specialized computing devices, this risk has increased. Multiple security experts and university research teams have shown that a threat actor could alter a voting machine’s configuration file to tamper with the vote count in a small amount of time, if given physical access to the machine [5] [6].

B. Notable Vulnerabilities Found in a Particular OS Machine

Diebold’s AccuVote Optical Scan (AV-OS) was a popular OS voting system that was investigated by researchers.

They attempted to infiltrate the machine with no internal knowledge of the hardware or software and no elevated privilege. They found that a simple lock holds the device in its protective housing, which could be opened very quickly. Pulling the terminal forward would reveal a RS-232 port on the rear side, which could then be attached to a mobile computer. Rebooting the system into diagnostic mode would allow an attacker to dump the memory card contents to the attacker’s computer via the serial cable without password authentication. The memory would be transmitted in cleartext, and the supervisor PIN could be extracted easily. This would allow the attacker to reconfigure the device and change the voting software and voting tally. After all changes are made, the logs would be altered to remove any trace of intrusion, and the device could be put into service [6].

Because this system is so similar to the legacy voting system, the security concerns are relatively minor compared to the alternatives.

C. DRE Machines

Direct Recording Electronic machines record votes via electronic means with no physical medium required. In 1974, the first DRE voting system was used in a general election. This system had voters use a coded voting card and a touchscreen to cast a vote that was stored in the machine and tabulated with the rest at the end of the poll [7]. These machines are typically linked via local area network and possibly via internet to a central tabulation computer.

Because of the electronic nature of these machines, their flexibility and cost savings quickly become evident. DRE machines have the possibility of accommodating many different handicaps that voters may possess with peripherals or software updates, increasing the privacy of the voters.

DRE machines also eliminate the need to print and distribute ballots. This is a significant cost in the voting system and requires considerable administrative overhead for proper distribution. Also, for elections that have to accommodate multiple languages, a simple software update can allow a machine to display any language necessary. This feature addresses availability concerns.

The main concern and vulnerability with this system is its main feature: the lack of any physical ballot for auditing or recount purposes, with the implication that a digital intrusion or loss could leave no trace of the actual votes cast on a machine. This puts an enormous burden on the security design of any implemented system, and as shown below, that responsibility has not always been taken seriously.

D. Diebold AccuVote-TS Machines

Diebold owned the most popular DRE voting machine in the United States in the 2000s. Security researchers from Princeton University were granted access to the most widely distributed model by an election official that wanted outside verification of the devices, and their results were alarming.

Researchers found many potential exploits that attackers could use to influence an election. For instance, voters could program their own smartcards (voter identification for the machine) that would allow multiple votes to be cast. This could be accomplished without access to the machine source code [8].

They also found that an attacker could cause serious damage with one minute of access to the machine. In that time, the security lock could be picked and access granted to
the PCMCIA memory card slot. From that point, they demonstrated that malicious software could be introduced that would modify all records, audit logs, and counters to alter the outcome of a vote without leaving a trace. A virus introduced by this method could infect other voting machines at the poll because of their unprotected network configuration. The attack could be done before, during, or after a poll with the same affect. They also found that, while some of the vulnerabilities could be addressed with changes to the hardware, software, or procedures, others were inherent and would require a new voting system to remedy [8].

Fig. 3. Diebold’s AV-TS voting terminal. As of 2010, this machine was being used in 1,400 jurisdictions in 33 states.

E. AVS WINVote Machines

One of the most troubling implementations of an electronic voting system ever found is the WINVote electronic voting machines, created by Advanced Voting Systems. These systems were in use in Virginia, Pennsylvania, and Mississippi. The Virginia state government audited the devices because of errors noted in the 2014 general elections, and numerous flaws were found [9].

Fig. 4. The AVS WINVote EVM, a machine that sources claimed could be hacked with a smartphone.

Physically, the device security was substandard. Several USB ports were protected by a cheap lock, while several more were physically open and able to accept almost any device. Researchers were able to alter the BIOS and boot the system from an external device easily [9].

The network security was the most alarming feature of this device. Each machine had an integrated 802.11b network card that was enabled and broadcasting the network SSID. The encryption algorithm used by the machine was the defunct WEP algorithm, and tests showed that disabling the wireless cards made the machines unable to perform their election functions. Several minutes of communications monitoring allowed the researchers to craft a network packet that cracked the password. The weak phrase “abcede” was hard-coded into each machine’s wireless settings [9].

The devices were all running Windows XP Embedded 2002 as the operating system, and they had not been patched since at least 2004. Researchers used a brute-force attack on the Administrator account and found the password almost immediately, “admin”. This gave them full access to the WINVote software [9].

The voting data itself was stored in a password-protected Microsoft Access database. A password cracker program guessed the password within 10 seconds, “shoup”. Researchers were able to modify the simulated voting data within remotely, without the knowledge of the election officials [9].

Jeremy Epstein, a security expert who viewed the report said, “If an election was held using the AVS WINVote, and it wasn’t hacked, it was only because no one tried [10]”. As a result of the investigation, Virginia decertified the AVS machines for election use. The other states followed suit.

The DRE machines, because of their network-centric design, need to have cyber security as a major element during their construction. The removal of the need to physically interact with a machine during an attack is a major advantage to the attacker, and it must be considered.

IV. ELECTRONIC HOME VOTING

The next evolution in voting is the inevitable conclusion in the electronic voting progression: electronic home voting. This process would allow a user to vote from any location on earth, provided an internet connection was available.

The benefits of this system are many and impactful. Election commissions would no longer be responsible for the logistical load or costs involved with coordinating locations, machines, officials, auditors, etc., to support elections. Absentee voters could simply vote from an internet-connected computer anywhere in the world. Multiple language formats could easily be accommodated, and handicapped people could use their own computers to vote instead of public terminals.

In order to satisfy the basic requirements of a legitimate vote, the security scenario is a familiar one to cyber security personnel: a verified user must be allowed to cast exactly one vote via a secure channel which is then securely stored and tabulated with the other valid votes. This process should also support audits by election officials and independent reviewers.

A. Versions Currently In Use

B. Major Concerns
V. POTENTIAL DAMAGE INFLECTED THROUGH ATTACK

Because of the attractive attributes of e-voting, it is possible to observe early adopters and learn from their mistakes. This is an important measure, because the perception of a valid voting process is more important to the voting public than an actual sound process.

Obviously, the systems with the largest risks involve those that leave no physical record of a vote. The purely electronic systems must have more secure protocols in place, and the ones that use the Internet are subject to persistent, world-wide attack possibilities from an array of adversaries.

Electronic voting, even that which occurs online, can be secured to a reasonable degree. This is demonstrable by the fact that banking, e-commerce, and myriad other functions containing sensitive data are currently performed online. A threshold of security needs to be established and enforced on any given election system.

There has been no known large-scale or pivotal exploit of the existing e-voting solutions, but the potential of such an attack is devastating.

Criminal enterprises could possibly muster the resources to affect the results of a local election with little or no trace. Nation-state level threats could alter or disrupt election operations on a national level, weakening the legitimacy of an elected government.

The 2000 U.S. presidential elections show how precarious the stability can be of even a democratically elected government of a prosperous nation if the system is attacked during administration change. That scenario involved lawsuits, accusations from both sides, and a Supreme Court ruling, all of which nearly paralyzed the national government for two weeks and weakened legitimacy. If something like that were to happen again, with the added complication of an e-voting breach and no physical back-ups, the winners would have a hard time establishing their power base outside their immediate supporters.

REFERENCES