IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Election Security through ElectionGuard

Dimple Gajra
Security Engineer, WA, USA

Vraj Patel
Security Engineer II, WA, USA

Sahil Dhir
Senior Risk and Security Manager, VA, USA

Suman Deep
Technical Architect, CA, USA

Keyur Rajyaguru
Intrusion Analyst, MD, USA

Abstract : This paper talks about the security aspect of Elections in the USA. The answers to questions like which kind of election voting machines are used, the security features of voting machines in general, and secrecy & privacy of votes can be found in this paper. This paper describes how ElectionGuard can be utilized to maintain end to end security of the election process.

INTRODUCTION

Election security refers to the measures and practices put in place to protect the integrity, confidentiality, and accuracy of election processes. This includes safeguarding all components of the electoral system, such as voting machines, databases, infrastructure, and communication networks, against threats that could compromise election outcomes or voter data. Key aspects of election security include:

Confidentiality: Ensuring that votes remain private and cannot be linked to individual voters, thereby protecting voter anonymity.
Integrity: Preventing tampering, alteration, or manipulation of votes and ensuring that each vote is accurately recorded and counted.
Availability: Guaranteeing that voters have reliable access to voting systems without interruptions or denial of service, even in the face of cyber threats.

Transparency and Verifiability: Implementing methods that allow voters, auditors, and election officials to verify that votes are cast and counted correctly without compromising security.

Protection from Disinformation: Safeguarding the process from misinformation and disinformation that could influence voter perception or behavior.

There are various methods to manipulate or influence election results. The Disinformation technique can be used to influence results and lure voters before they vote. This can be done by various techniques like building a bot on any social media and spreading fallacious information. Spreading incorrect information multiple times on social media will make people believe that the information is true, and they will start believing it. Campaigners also use targeted advertising to manipulate voters. They build a profile on their target audience based on their likes, dislikes, age, social media presence, their expectations, and other multiple data points from various other sources. Campaign data, including certain public information on campaign donations, is available through legitimate sources like Political MoneyLine and other transparent, regulated platforms. The decisions of those users influence the decision of their friends, family, and acquaintances. And due to the domino effect, the end goal is changed. In the Cambridge Analytica campaign, 87m records scraped from Meta allegedly changed the election results. Cash was provided as an incentive to influence users to fill a form and submit data. Those data points were used to target voters. Similarly, social media bots were used to spread information. This can be detected by looking out for fake accounts, the rate at which an account is tweeting, the secrecy of an account, the amount of private information revealed from that account, a sudden spike in account activity, number of followers and the accounts followed by the fake account, looking for applications and accounts collecting a lot of data, analyzing advertisements on social media and the owner of those advertisements. Meta analyzes every account to check if it is fake or real and is checking all the applications to check which kind of data is shared with them, many social media platforms also banned political advertisements and are continuously looking for bots. So, to prevent elections to be influenced beforehand, there should be campaigns to educate voters on distinguish between misinformation and factual information. There can be websites to verify truthful information related to elections.

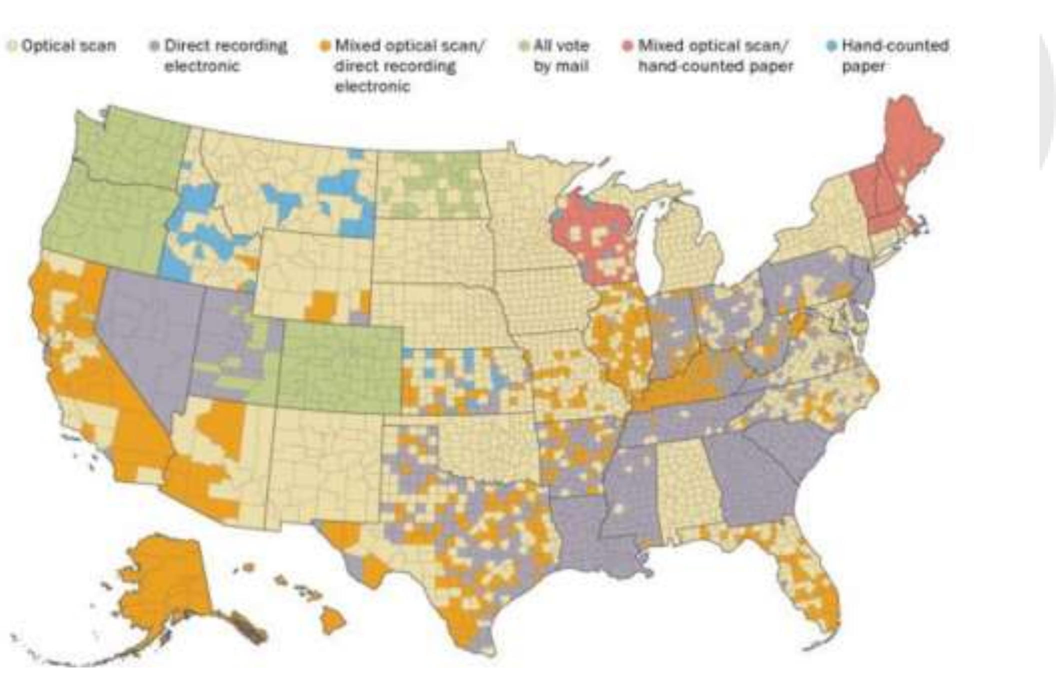
During the voting process, there are various security aspects that need to be considered. Voting machines can be subverted by manipulating OS, firmware, the hardware of the machine, exploiting common vulnerabilities, and subverting the supply chain.
It is important to do threat modeling before designing any voting machine to determine where the attacker can come from and what can they do and how can it be prevented. In its designing and development stage, Security and Privacy by design approach should be followed. Another important factor to consider is vulnerability management. Chain of custody of all voting machines and assets should be maintained during the whole election process, before and after it as well. Sometimes, the machines are powered off and go off the radar which remains vulnerable and unpatched. Pen testing of machines should be done in a production environment. Mock elections can be conducted to test the whole process, and physical security of the election zone should be of importance. The badges of Election officials should difficult to clone. The teams handling the process at each booth should consist a minimum number of members possible, so it becomes difficult for an external entity to infiltrate the team and perform any malicious activity. Every member should not have access to each and every activity going on in the whole voting process, and access to the process in different facilities as well, least privilege principle should be followed by granting them individual roles.

There are three aspects of ensuring security in voting machines. Votes should remain confidential, tamperproof, and available to be verified anytime. The machines should be easy to use for everybody.

Aspects considered for verifiability:
Individual: Allows a voter to verify that the vote is included in the final counting
Universal: Allows voter or election observers to check that the election outcome corresponds to the votes casted
Eligibility: To verify each vote was casted by a unique user
To audit any system a strict chain of custody is required. If we can confidently establish that who accessed the machine at what time and the machine was not left unattended, we can firmly establish the proof that there was no unauthorized access physically and no one tampered the ballot. Auditing provides proof to losing candidates, the winner, public, and election officials that the results were accurate and efficient.
Assurance in the voting machine can be provided by answering the following questions:

- Where is the TPM in the voting machine? What keys are stored in it and who has access to it? When does the key leave the TPM?
- How is the signing of the voting software done? Who does it?
- Who has access to the software source code?
- How can we trust the CA?
- Is every voter a Unique user?
- How is the verification of the vote done?

Currently Used Methods to Cast a Vote


Optical scan
Direct recording electronic
Mixed optical scan/ direct recording electronic
All vote by mail
Mixed optical scan/ hand-counted paper
Hand-counted paper

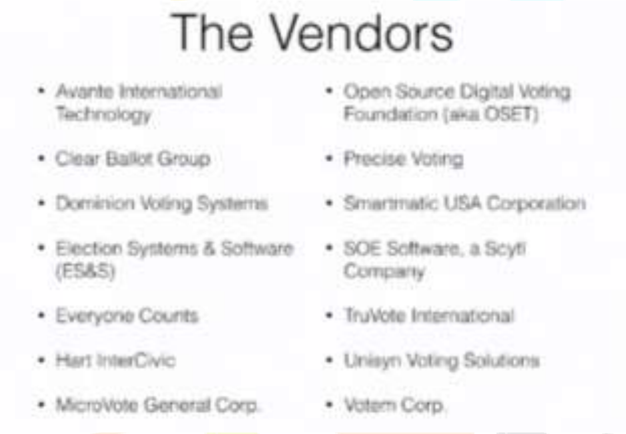
Optical Scan Paper Ballot Systems: Voters mark their votes by filling in an oval, box, or similar shape on a paper ballot. The paper ballots are scanned either at the polling place or a central location. [10]

Direct Recording Electronic (DRE) Systems: DRE systems employ computers that record votes directly into the computers' memory. These interfaces may incorporate touchscreens, dials, or mechanical buttons. The voter's choices are stored by the computer on a cartridge or hard drive. Some DRE systems are also equipped with a printer, which the voter may use to confirm choices before committing them to the computer's memory. [10]

Ballot Marking Devices and Systems: These systems are designed to help disabled voters who might be unable to vote using other methods. Most devices utilize a touchscreen along with audio or other accessibility features. Rather than recording the vote into the computer's memory, the ballot is instead marked on paper and later tabulated manually. [10]

Punch Card Voting Systems: These devices employ a paper card and a small clipboard device. A voter punches holes in the card to mark his or her vote. The pattern of holes in the card indicates the votes cast. The ballot may then be placed in a box to be tabulated manually or scanned by a computer later. [10]
Additionally, remote options like mail-in voting are available in many states, expanding accessibility for voters who may not be able to vote in person.

The U.S. voting machine landscape is largely served by major vendors like Dominion Voting Systems, Election Systems & Software (ES&S), and Hart InterCivic. These vendors supply the majority of voting equipment used nationally, although other smaller, regional vendors also contribute..



The Vendors

- Avante International Technology
- Clear Ballot Group
- Dominion Voting Systems
- Election Systems & Software (ES&S)
- Everyone Counts
- Hart InterCivic
- MicroVote General Corp.
- Open Source Digital Voting Foundation (aka OSET)
- Precise Voting
- Smartmatic USA Corporation
- SOE Software, a Scytl Company
- TruVote International
- Unisyn Voting Solutions
- Votem Corp.

The problems with the current system are that it is difficult to check if the machine was hacked, or the replaced or the voter's vote was counted as submitted. The systems are not the open source to be able to be verified. Security evaluations of existing systems have revealed that attackers can forge or alter results, install corrupt firmware, and erase audit logs. To overcome all the problems, Microsoft has launched the end to end verifiable voting system.

ElectionGuard

ElectionGuard, an open-source solution from Microsoft, offers end-to-end verifiability to ensure secure, transparent elections. It makes voting secure, transparent, accessible, and end to end verifiable. It uses homomorphic encryption to safeguard votes, allowing individual votes to be encrypted while enabling the accurate tally of totals without decryption of individual selections. This encryption maintains voter privacy and supports election transparency

ElectionGuard provides each voter with a unique tracking code, allowing voters to verify their vote was included in the tally without revealing individual choices. It also enables independent audits by external observers, enhancing transparency. Since its launch, ElectionGuard has been tested in pilot programs across jurisdictions, such as in Wisconsin, where it demonstrated compatibility with traditional paper-based voting systems.

Key elements in ElectionGuard include:

- Homomorphic Encryption: Ensures that votes are private yet countable in aggregate.
- Risk-Limiting Audits (RLAs): ElectionGuard's encrypted vote tallying is compatible with RLAs, used to verify digital results with physical ballots.
- Independent Verifiability: ElectionGuard's open-source nature allows third parties to audit results and verify vote counts, increasing public trust in the electoral process.

Future updates include potential support for ranked-choice voting, which is under development.

Terminology:

- Election Officials: Individuals responsible for administering the election process, which includes managing polling sites, verifying voter eligibility, and ensuring accurate vote tallying. Election officials may include members of canvassing boards, poll workers, county clerks, and judges, with responsibilities varying by jurisdiction.

- Guardians: In ElectionGuard's framework, Guardians are individuals designated to manage and secure cryptographic elements, such as encryption keys. Guardians play a crucial role in upholding election security by enabling independent verification while ensuring vote privacy. Their responsibilities include collaborating to decrypt tallies and ensuring no single person can alter election outcomes without consensus.

- Voter: An eligible member of the public who participates in an election by casting a ballot.

- Ballot Encryption: The process of converting a voter's choices into an encrypted form to ensure privacy and security. ElectionGuard uses homomorphic encryption to allow votes to be counted without decrypting each individual vote, preserving voter confidentiality while enabling accurate tallying.

- Tracker Code: A unique code generated for each voter that allows them to confirm their vote was included in the final tally. This code does not reveal the contents of the vote, ensuring privacy while providing verifiability for individual.
- Homomorphic Encryption: A form of encryption that allows operations to be performed on encrypted data. In ElectionGuard, homomorphic encryption enables encrypted votes to be tallied without revealing individual choices, maintaining both privacy and transparency.

- Risk-Limiting Audit (RLA): A post-election audit method that confirms election outcomes by statistically sampling ballots. ElectionGuard is compatible with RLAs, enhancing verification by allowing comparison of physical ballots with digitally encrypted votes.

- Election Record: A public record generated after an election that contains encrypted vote data, cryptographic proofs, and other information. This record allows independent verification of results by external parties without compromising individual voter privacy.

Types of computers and application involved in the process:

Key Generation Application/Device: Generates cryptographic keys essential for securing the election process. It coordinates with Guardians to create and distribute election keys while preventing any single entity from having complete control.
Guardian Application/Device: Managed by designated Guardians who handle cryptographic keys. These devices ensure encryption and decryption of votes and require collaboration among multiple Guardians to maintain data security and prevent unauthorized access.

Ballot Marking Device (BMD): Provides a touchscreen interface for voters to make selections privately. It produces a paper ballot summary and a tracker code, allowing voters to verify their votes post-election. BMDs are air-gapped from the internet to prevent external interference.

Election Controller: Located at each polling site, this device verifies voter eligibility, manages ballot styles, and marks ballots as spoiled when necessary. It can also confirm encryption status to assure voters of secure vote handling.
Ballot Box Application/Device: Functions as a secure, electronic ballot box that records each vote cast, confirming eligibility and excluding spoiled ballots from the final tally.

Verification Portal (Web Application): Allows voters to check that their votes were counted in the final tally using a tracker code. This portal is typically made available publicly post-election, providing transparency and verifiability.
Tally System: Processes encrypted votes, leveraging homomorphic encryption to calculate election results without decrypting individual votes, thus maintaining voter privacy while ensuring an accurate count.

Figure 3 Sequence Diagram : Election Guard

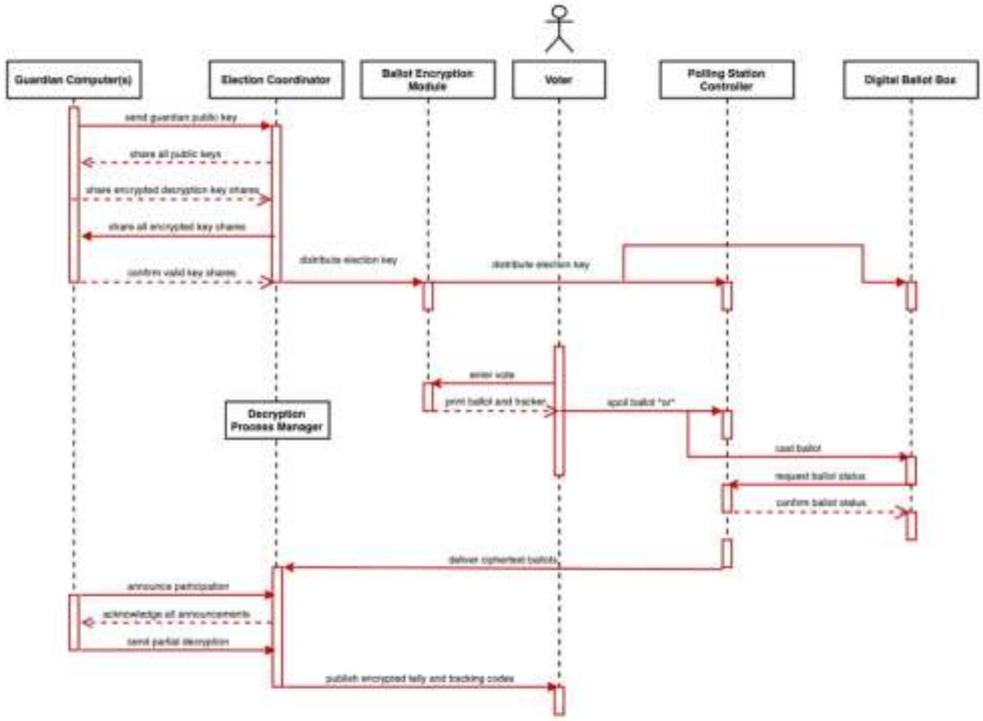
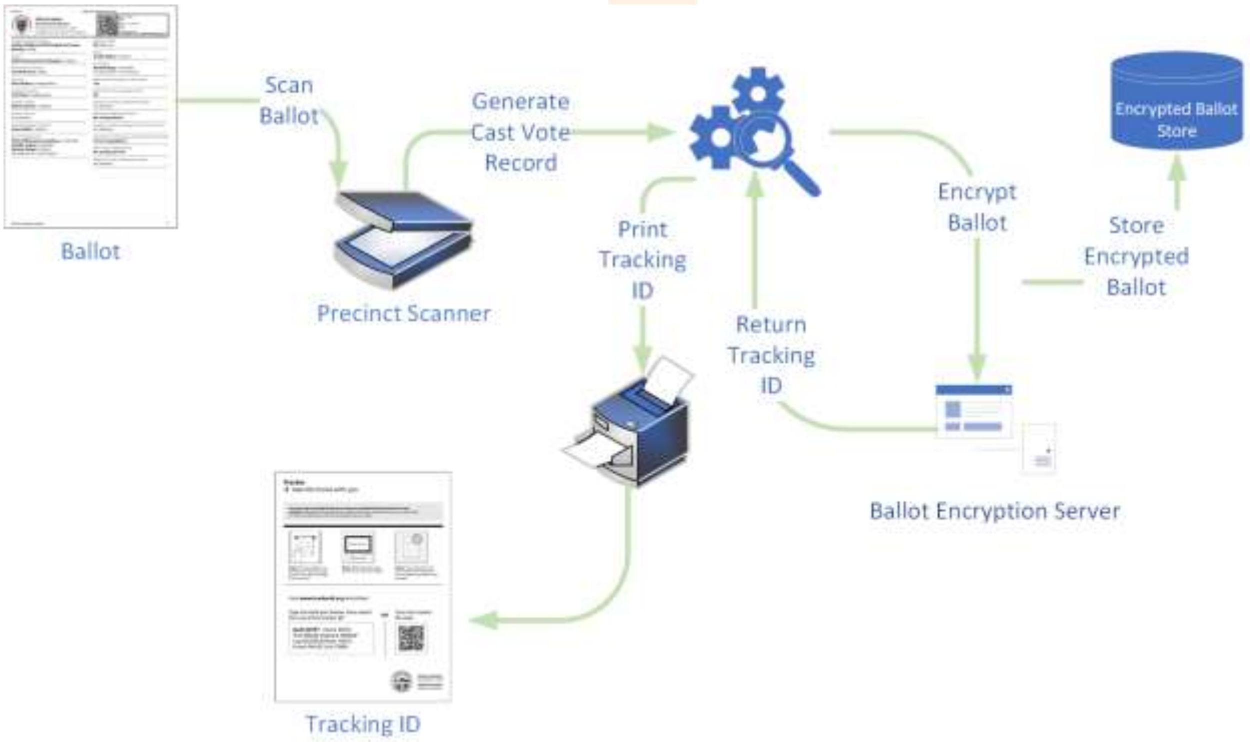


Figure 4 Voting system



The election process using ElectionGuard begins with Guardians (formerly referred to as Trustees) generating public-private key pairs to establish a secure foundation for vote encryption. These Guardians play a crucial role in maintaining data security by ensuring that control is decentralized and no single individual can access or manipulate vote data alone. Multiple Guardians must collaborate to decrypt votes, thereby ensuring transparency and trust in the process. Guardians create individual public-private key pairs, which are then combined to generate a shared election public key used to encrypt each voter's ballot. To authenticate their participation without compromising security, each Guardian provides a Schnorr Proof — a cryptographic proof that confirms the authenticity of their private key without exposing it. This system ensures that the encryption keys are genuinely from trusted sources.

To enhance fault tolerance, each Guardian's private key is split and distributed among all Guardians using Shamir's Secret Sharing or a similar cryptographic technique. In this arrangement, only a subset of Guardians is required to reconstruct a missing key, ensuring the process can proceed even if one Guardian is unavailable. Once key generation is complete, the Guardians' computers share their public keys with the Ceremony Coordinator, who combines them to produce the final election key. This key will later be distributed to all components involved in the voting process. A Zero-Knowledge Proof is used to validate the integrity of each key without revealing any private information. This proof includes a hash of all election parameters, providing a way to confirm that the keys were not tampered with.

On Election Day, the voter arrives at the polling station and undergoes a standard authentication check (e.g., identity verification). Once authenticated, the voter is issued a token — typically a smartcard or a PIN — that links them to their specific ballot style and ensures that they can only vote once. After receiving their token, the voter casts their ballot using a Ballot Encryption System, which encrypts the vote using the election public key. This system generates a unique tracking code for each voter, enabling them to verify that their vote was included in the final count without revealing how they voted. To further enhance transparency, the system prints two receipts for each voter: one containing their encrypted ballot information and another with a verification barcode. This dual-receipt system allows the voter to confirm that their vote was counted, although it can sometimes lead to confusion among voters.

After the ballot is encrypted, it is broadcast as a data packet over a secure local network, typically air-gapped to prevent unauthorized access. This packet contains the encrypted vote, the unique voter ID, and the Cast Vote Record (CVR), allowing for reliable tracking and verification. At this stage, the voter has the option to either finalize their vote or spoil the ballot. Spoiled ballots are marked for separate handling and are decrypted after the election to confirm they weren't mistakenly included in the tally.

Once voting is complete, each encrypted ballot is submitted along with a Non-Interactive Zero-Knowledge Proof, verifying the authenticity of each vote without revealing its content. The encrypted ballots are then combined using homomorphic encryption, allowing the tally to be calculated without decrypting individual votes. The Guardians' role becomes essential again as they perform partial decryption of the votes using their private keys. This collaborative decryption process ensures that the final tally is transparent and tamper-proof. These partial decryptions are then combined to reveal the overall tally, which is published for public review.

For additional transparency, all encrypted votes, along with their tracking codes and verifiable proofs, are made available in a downloadable file (e.g., .zip format). Independent auditors and the public can access this data to confirm the integrity of the election. New encryption keys are generated for each election to prevent any unauthorized access, and if any Guardian leaves, the entire encryption setup is reset. Throughout the election, all sensitive processes, including key sharing, are conducted on air-gapped devices to ensure security.

Homomorphic encryption plays a crucial role in ElectionGuard, allowing individual votes to remain private while enabling accurate aggregation. This type of encryption allows mathematical operations on encrypted data, meaning that the final tally can be computed without decrypting each individual vote. Additionally, homomorphic encryption has verification properties that confirm the accuracy of the tally and ensure that each voter selected only the permitted number of options. Tracking codes are securely stored, preventing unauthorized access, although they could theoretically be linked to a voter. Thus, special protocols ensure that these codes remain confidential.

After the election, the ElectionGuard API enables auditing, providing comprehensive checks to confirm the security and accuracy of the election process. The API validates key aspects, such as Guardian participation in decryption, integrity of election keys, accuracy of the vote tally, and transparency in public records. This level of verification ensures that the election results are trustworthy and accurately reflect the will of the voters. By combining Guardian collaboration, cryptographic proofs, homomorphic encryption, and public verifiability, ElectionGuard establishes a robust and transparent election system that upholds both voter privacy and election integrity.

Verification	Implication
Number of Guardians (formerly Trustees) able to decrypt the election > 0	Confirms end-to-end security, ensuring that only authorized Guardians can decrypt results together.
Threshold of Guardians required to decrypt the election > 0 and < Total number of Guardians	Prevents any single Guardian from decrypting or altering results, enforcing collaborative security.
Encryption parameters (prime modulus and group generator) validity	Ensures that the encryption keys are from authorized sources and meet security standards.
Hash of election parameters computed correctly	Confirms the integrity of encryption parameters used in securing votes, ensuring no tampering.
Extended base hash computed correctly	Verifies the integrity of all public keys shared among Guardians, ensuring each comes from a trusted source.
Joint public key computed correctly	Confirms that all Guardian public keys are correctly integrated, establishing an accurate election key.

- ElectionGuardians’checks:

Verification	Implication
Guardian public keys = number of Guardians	Verifies that each Guardian's key is legitimate, ensuring no unauthorized keys have been added.
Correct number of coefficients in each Guardian’s public key	Confirms each Guardian’s key is set up correctly for threshold decryption, protecting election integrity.
Guardian possesses a private key matching their published public key	Confirms the private-public key pairing, ensuring keys belong to legitimate Guardians and not attackers.

ElectionGuard’s Zero-Knowledge Proofs (ZKPs) ensure that Guardians can confirm their identities without revealing private key details, bolstering system integrity and privacy.

- **Cast ballot** checks:

Number of contests = number of contests specified for the election	Confirms that ballots meet election standards, ensuring all contest details are correct.
The number of possible selections for each contest = number of possible selections specified for the election	Ensures that each voter’s selections meet the contest rules, preserving vote integrity.
The voter selected no more than the total permissible number of selections for that contest	Prevents over-voting, validating that each ballot complies with election rules.
For each contest, any given selection corresponds to either one or zero votes	Confirms accurate, binary recording of each vote selection for clear and reliable vote counting.

- **Spoiled ballot** audit:

Verification	Implication
Number of contests = the number of contests specified for the election	Confirms that the ballot structure aligns with the election setup, preserving ballot integrity.
number of possible selections for each contest = the number of possible selections specified for the election	Validates that voters didn’t exceed selection limits, ensuring accurate representation.
The encrypted ballot decrypts to the cleartext ballot that accompanies it	Verifies the vote as cast, ensuring the voter’s intent is accurately recorded.

- **Published final tally** checks:

Verification	Implication
The encrypted sum calculated from the individual ballots = encrypted sum published in the election record	Ensures that all recorded votes are accurate, confirming vote integrity
The encrypted sum published is an encryption of the published cleartext result of the election	Confirms that published results reflect the actual votes cast, maintaining transparency and trustworthiness.

Encrypted ballots are randomly selected and compared against physical ballots to obtain confidence that the physical records match the electronic records.
ElectionGuard verifies all the steps in the process from key generation, its parameters, voting process, and vote counting which builds trust amongst everyone that the elections were not tampered with.

Things not covered by the ElectionGuard:

- Provisional Voting: ElectionGuard lacks support for provisional ballots, which are used when a voter's eligibility must be verified post-election. This feature is critical in many election processes to ensure all eligible votes are counted.

- Ranked-Choice Voting: ElectionGuard does not yet support ranked-choice voting, a voting method where voters rank candidates in order of preference. This method has grown in popularity in certain jurisdictions but requires more complex tallying algorithms than ElectionGuard currently accommodates.

- Key Management and Sharing: ElectionGuard provides the framework for secure elections but does not prescribe specific key management or sharing protocols. This responsibility falls to local jurisdictions or vendors implementing ElectionGuard. They must establish secure key custody, rotation, and distribution practices to ensure compliance with ElectionGuard's security standards.

This whole software will give control to the authorities to conduct elections in a secure manner. The government can buy a Secure hardware module from the third party and ask them to embed this software to conduct secure ballots. This will provide the assurance that the code is reviewed and verified. Many third-party vendors don't provide an option to the government to review the code. It is not impossible to hack the machine, but when a machine is hacked it becomes more obvious and prominent when ElectionGuard is used. One another issue with the ElectionGuard system is, it is open source and anyone can have access to it and exploit it. There are still many old OS running on voting machines, so to run ElectionGuard they must be replaced and recertified creating an overhead and burden on the committee.

Apart from the recent technology above, DARPA has funded for developing a System Security Integration Through Hardware & Firmware (SSITH). It is integrated with the BESPIN voting system (BVS) to demonstrate the SSITH. BVS is a software that provides functions of a voting system. The BVS was just developed as a proof of concept for SSITH. BVS is not end to end verifiable. ElectionGuard can be integrated with SSITH to ensure that the keys won't be leaked through memory vulnerabilities and are secured with the Secure hardware module. SSITH holds secret keys in DRAM while they perform encryption, decryption, and secret key-based hashing. Voting machines used today rely on paper ballots to detect hardware-based errors. SSITH will solve that problem and prevent attacks at the hardware level.

References

1) https://github.com/GaloisInc/BESSPIN-Voting-System-Demonstrator-2019
2) https://arxiv.org/pdf/1504.03778.pdf
3) https://arstechnica.com/information-technology/2008/02/analysis-evotings-success-rests-on-chain-of-custody-issue/
4) https://en.wikipedia.org/wiki/Electronic_voting
5) DEF CON 26 VOTING VILLAGE - Joseph Kiniry - Trustworthy Elections
6) Tod Beardsley - Securing Voting Systems Beyond Paper Ballots - DEF CON 27 Voting Village
7) DEF CON 25 Voting Village - Harri Hursti - Brief history of election machine hacking
8) https://people.csail.mit.edu/rivest/pubs/Riv19g.pdf
9) https://www.essvote.com/products/expressvote/
10) https://ballotpedia.org/Voting_methods_and_equipment_by_state
11) https://github.com/microsoft/electionguard-verifier
12) https://pages.nist.gov/ElectionGlossary/#contest-option
13) https://www.cnet.com/features/this-could-be-microsofts-most-important-product-in-2020-if-it-works/
14) https://www.usenix.org/legacy/event/evt08/tech/full_papers/aviv/aviv.pdf
15) https://securehardware.org/FAQ/
16) https://www.youtube.com/watch?v=tGRPYVRZ7pU
17) https://www.electionguard.vote/overview/Glossary/#other-terms-election-guardian-missing-guardian-available-guardian