CIS Center for Internet Security®

How to Improve Election Technology Verification

A Proposal for Rapid Architecture-Based Election Technology Verification (RABET-V)

Aaron Wilson • Sr. Director of Election Security • aaron.wilson@cisecurity.org

Summary

The Problem

There is no standard process for verifying that non-voting election technology is secure, reliable, and usable. This puts elections jurisdictions at risk, burdens vendors with extra costs, and risks inconsistent and insecure outcomes. Existing election technology verification processes are costly, slow, and disincentivize updating products at the same pace as technology changes and security threats. More efficient verification processes exist but are not yet being leveraged for election technology.

The RABET-V Solution

RABET-V is an election technology verification process that supports rapid product changes using a risk-based approach. Rather than reviewing the entire system with each change, the re-verification of documented and well-architected systems should only evaluate system aspects which are effected by the change.

A successful implementation of the RABET-V approach would have four primary benefits:

1. Incentives for high-quality, modern design of IT systems that are more resistant to attacks and more resilient in recovery;
2. Incentives to update in smaller, more manageable cycles, more accurately reflecting the modern age of software development;
3. Reduced cost of verification and re-verification and more reliable and consistent outcomes for purchasers of the systems; and
4. A consistent basis from which approval authorities (namely states) can draw information, resulting in quicker decisions and reduced, amortized overall cost.

The RABET-V Approach

RABET-V initially creates a baseline of security claims and product assertions that are informed by a thorough product review that assesses architecture robustness and the maturity of the processes used by the technology provider. The product is then tested to verify that the security claims are met and the results are acceptable.

In subsequent system upgrades, the developer submits a description and software for proposed changes and, using the product assertions as a guide, the evaluation verifies the aspects of the system most likely to be impacted by the revision. This results in more rapid and less costly verification which encourages more security and functional improvements.

We are convening a group of election officials, technology providers, and other election stakeholders to develop and conduct a RABET-V Pilot Program and evaluate the RABET-V process.

Background and Motivation

There is currently no standard process for verifying non-voting election technology.[1] Some states, including California, Indiana, Florida, and Ohio have defined their own unique verification processes. These state processes are modeled after voting system verification processes which result in a costly and time consuming approach that begins with the submission of large volumes of documentation, hardware and code to an independent lab and concludes many months later with a formal test report and, if approved, signoff by authorities.[2] The full process is repeated for any subsequent verifications required for system changes or upgrades, such as a security update. It is a people- and paper-intensive process that is slow, costly, and rigid.

Non-voting systems are typically built using commercial hardware and software components that may receive regular security patches and updates. These systems must adapt quickly to changes in the threat and usage landscapes and therefore require a verification process that supports this rapid change. The existing verification processes disincentivize product change and innovation, resulting in election information systems often running outdated and unpatched software.[3]

The existing verification processes also differ greatly from modern software development, which delivers incremental additional or improved functionality to users on a regular basis. Increasingly, testing is fully automated. Moreover, developers use architectural models that enable modular system upgrades and focused system testing (e.g., if the impact of a change is localized to one part of the architecture, only that portion of the code is retested). There are also third-party assessment tools available for architecture, design, and code analysis as well as for internal and independent testing.

RABET-V is designed to take advantage of these modern software development, testing, and deployment practices and tools in order to provide a high confidence, flexible, rapid, and cost-efficient process for verifying non-voting election systems. High confidence is achieved by providing evidence-based assurances of system reliability and security while using independent testing only when necessary to complement the available system design artifacts and test results from developers.

[1] An election technology system is an information system that supports an election administration process. There are both voting and non-voting types of election systems. A "voting system" is defined in the Help American Vote Act (H.R. 3295, Sec 301). A non-voting system is any other election technology system used during the election. Examples include voter registration databases, electronic pollbooks, or the websites of government election authorities.

[2] The voting system testing and certification process varies by state. The Election Assistance Commission's (EAC) testing and certification process, which is incorporated into many state processes, is described in the EAC Testing and Certification Program Manual available at https://www.eac.gov/voting-equipment/manuals-and-forms

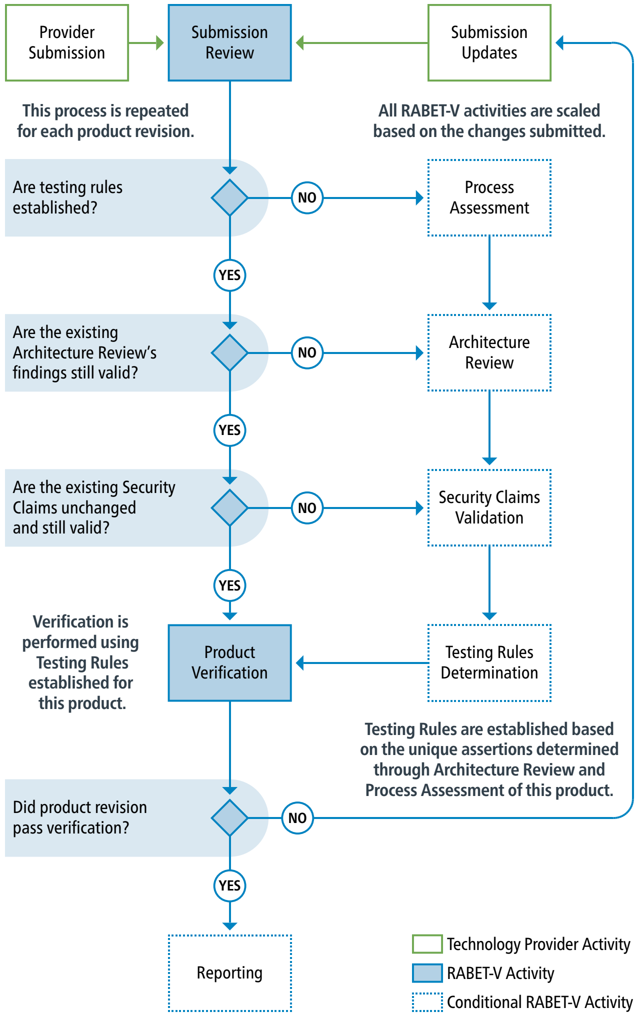
[3] According to *The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration* (pg. 64): "Even when it works as designed, the certification process is costly and burdensome. Vendors complain about the length of time and expense (well over $1 million for a new voting machine) of receiving certification from one of the few approved testing labs. Indeed, the certification process even retards improvement of existing, certified equipment as it requires additional certification for even small modifications or upgrades. As a result, the certification process simply does not fit with an election calendar. Because of the time it takes to discover flaws following an election, to develop a "fix," and then to have it certified, it is likely that the known solutions to problems discovered in one election will not be in operation for the next one."

RABET-V Process

The Rapid Architecture-Based Election Technology Verification (RABET-V) process consists of seven total activities, five of which are conditional activities that are scaled to meet the needs of the particular review. This scaling provides a rapid, risk-based testing strategy informed by the product's architecture, the developer's processes, and their security claims. This risk-based strategy is driven by unique Testing Rules for each product. The **Architecture Review**, **Process Assessment**, and **Security Claims Validation** activities provide assertions about the system's construction which inform the **Testing Rules Determination** activity. These Testing Rules are a set of assertions and conditions that will guide system testing in the **Product Verification** activity. The Testing Rules may vary based on the product and the provider. This approach will yield a rapid and cost-effective approach to determine whether the systems' security, reliability, and usability are acceptable.

The Testing Rules reflect the soundness of the system architecture and the design approach for security and other important system features (e.g., usability). Better system architectures and more mature internal software development processes yield a more time- and cost-efficient set of Testing Rules, creating incentives for sound development practices early on. Leveraging industry-leading best practices, RABET-V will maintain Technical Guidance describing the desired qualities and characteristics of favorable architecture approaches and development processes.

The RABET-V process is conducted for the initial submitted product version as well as each subsequent revision of the system. Each iteration of RABET-V evaluates the product changes during the **Submission Review** activity and adapts the overall review process based on the scope and potential impact of the changes. For changes that don't fundamentally alter the architecture of the product or its security claims, the process skips the conditional activities that define the Testing Rules and moves directly to **Product Verification** where the existing Testing Rules are used to evaluate the product changes. This provides an efficient way to conduct testing based on the risk to security, reliability, or usability assurances. To the extent possible, each RABET-V iteration is conducted in parallel to the provider's development cycle, collecting and assessing evidence along the way to expedite testing of each product version.


Provider Submission
Submission Review
Submission Updates
This process is repeated for each product revision.
All RABET-V activities are scaled based on the changes submitted.
Are testing rules established?
NO
Process Assessment
YES
Are the existing Architecture Review's findings still valid?
NO
Architecture Review
YES
Are the existing Security Claims unchanged and still valid?
NO
Security Claims Validation
YES
Verification is performed using Testing Rules established for this product.
Product Verification
Testing Rules Determination
Testing Rules are established based on the unique assertions determined through Architecture Review and Process Assessment of this product.
Did product revision pass verification?
NO
YES
Reporting
Technology Provider Activity
RABET-V Activity
Conditional RABET-V Activity

Provider Submission and Submission Review

The RABET-V process is initiated when the provider submits their product information. The initial submission will include product goals, expected usage, product security claims, architecture documentation and diagrams, process descriptions, and third-party component details. Subsequent product revisions will submit the updated system, operations and development artifacts, and a record of all changes. The technology provider may optionally submit updates to the initial submission, such as modifications to their security claims.

The Submission Review activity will then review the submission package to determine its adequacy and the right RABET-V activities to conduct. Products without established Testing Rules will go through each activity. Product revisions with minimal changes will move immediately to the Product Verification activity.

Security Claims Validation

Product security claims are statements of compliance with security best practices. This activity reviews the validity and efficacy of the providers' security claims to support their product's goals and expectations. Validated security claims will be published in the public domain. This transparency informs potential customers of the product's security claims which encourages providers to continually improve their security.

Architecture Review

The Architecture Review results in assertions about how the system should be tested.[4] The RABET-V architecture review includes four points of view to ensure the most important aspects are evaluated:

1. **System.** The system architecture review looks at the whole system and how the various layers of hardware and software components, third-party services and solutions, and election applications work together.
2. **Software.** The software architecture review looks at how the election application software is constructed with regard to partitioning of functions, allocation of system features, and the implementation approach for key security and system usability requirements.
3. **Security.** The security architecture review looks at how the system architecture is constructed to provide stated security capabilities.
4. **Data.** The data architecture review examines the system's data types, how that data is moved throughout the system and external to the system, which components handle sensitive data, and the formats used for the data.

Well-architected solutions will result in the maximum amount of assertions and shorter verification cycles. Poorly architected solutions will result in fewer assertions and longer reviews for subsequent changes.

Process Assessment

The RABET-V Process Assessment looks at the developer's software development lifecycle processes that are critical to maintaining the security, usability, and reliability of the system. Organizations will be assessed for their maturity and product changes resulting from organizations with more mature processes will be considered lower risk. It will also be easier for companies with mature processes to produce the artifacts required by the RABET-V testing.

Testing Rules Determination

This activity builds a set of Testing Rules to achieve the most rapid, flexible, and reliable testing of product revisions possible given the product architecture and provider's processes. For each type of change, specific test methods are prescribed commensurate with the risk introduced by the change. This allows, for the same level of resources, more focus on the areas for which risks might be introduced by the change without being distracted by areas that would be unaffected by the change. For well-defined architectures and mature processes, the testing may be minimal, automated, or deferred to the technology provider. Small change sets and security patches will receive the most expedited testing since risk-based decisions are more accurate for smaller change sets.

[4] According to the Software Engineering Institute, architecture evaluations result in the identification of design risks and assist in predicting system quality. Reduce Risk with Architecture Evaluation, Carnegie Mellon University Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/FactSheet/2018_010_001_515610.pdf

Product Verification and Reporting

The Product Verification activity follows a test plan created from the Testing Rules. Creating the test plan will be a quick, ideally automated, process of pairing up the product changes with test methods in the Testing Rules. For small, low-risk changes, the test plan may only be a review of the artifacts submitted by the developer. For larger, higher-risk changes, the test plan may require functional or other types of testing.

Product Verification will leverage product development artifacts that are reliable and indicative of product security. For example, the vendor could submit unit testing and vulnerability scan results. It can also include security event analysis, which will indicate the security threats the product is handling and how well its security controls are operating.

At the conclusion of Product Verification, the RABET-V process will publish the product goals, usage, verified product claims, and verified product changes.

Pilot Program and Open Questions

The RABET-V Pilot Program will evaluate and refine the RABET-V process and address open questions from both technical and non-technical perspectives. This effort will be guided by a Steering Committee comprised of election officials, election technology providers, and other election infrastructure stakeholders.

The RABET-V Pilot Program will first establish a detailed version of the RABET-V process called the RABET-V Working Model. This version will detail how each activity will be conducted. The Working Model will identify the initial Technical Guidance necessary to perform the Architecture Review and Process Assessment. The Working Model will be iteratively reviewed by the program Steering Committee and modified as necessary.

? There are several critical open questions to address while developing the Working Model. The first is how to incorporate usability and accessibility testing. We heard from the community that any verification process must incorporate these aspects in order to be viable. Second, the Working Model must address how to handle non-voting solutions built and maintained by election offices. Third, the Working Model should address which third-party accreditations will be incorporated.

Using the Working Model, the Pilot Program will conduct initial reviews on real products from Pilot Program participants. Each initial review will execute all seven RABET-V activities resulting in the creation of Testing Rules and initial verification results for each product. The Architecture Review and Process Assessments will follow the architecture and process review steps detailed in the Working Model, which may be updated as necessary throughout the Pilot Program. Along with evaluating the time and cost of each, the Pilot Program will evaluate the value of the Architecture Review, Process Assessment, and Security Claims Validation activities to determine appropriate Testing Rules.

? The Pilot Program will address open questions about product and provider maturity. We must determine if the product architectures and provider processes are mature enough to support RABET-V. Some key objectives of RABET-V hinge on the prevalence of well-defined architectures and mature processes. The pilot will assess the potential of giving feedback to product developers to improve weaknesses in system architectures and development processes.

The Pilot Program will then conduct multiple iterations of RABET-V on product revisions from the participants. Depending on the changes, RABET-V will adapt and conduct only the activities required. This exercise will highlight the effectiveness of RABET-V to create meaningful but streamlined verifications and help determine the effectiveness of the product architecture and process reviews. It will also provide useful time and cost information. After each RABET-V iteration, changes may be made to the testing process and the iteration repeated as necessary.

? The Pilot Program will address open questions on how well RABET-V can establish rapid, flexible, and cost-efficient testing rules for future product revisions. The process must also determine the level of architecture and process maturity necessary for the speed and cost improvements to be consistently realized.

About The Center for Internet Security (CIS)

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously refine these standards to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

Contact

Center for Internet Security
31 Tech Valley Drive
East Greenbush, New York 12061

www.cisecurity.org
info@cisecurity.org
518.266.3460