The Center for Internet Security would like to thank the Democracy Fund for its generous support of the RABET-V pilot.

RABET-V Pilot Update and SolarWinds Mitigations

Aaron Wilson, Sr. Director of Election Security

Rapid Architecture-Based Election Technology Verification (RABET-V) Pilot Status

The Rapid Architecture-Based Election Technology Verification (RABET-V) is an election technology verification process that supports rapid product changes by design. Having completed the first pilot phase, it has achieved its goal of developing a verification process for election technology that matches the environment of modern software development, particularly for systems for which a continually-evolving threat space—and thus approach to risk mitigation—dictate a shorter technology deployment cycle.

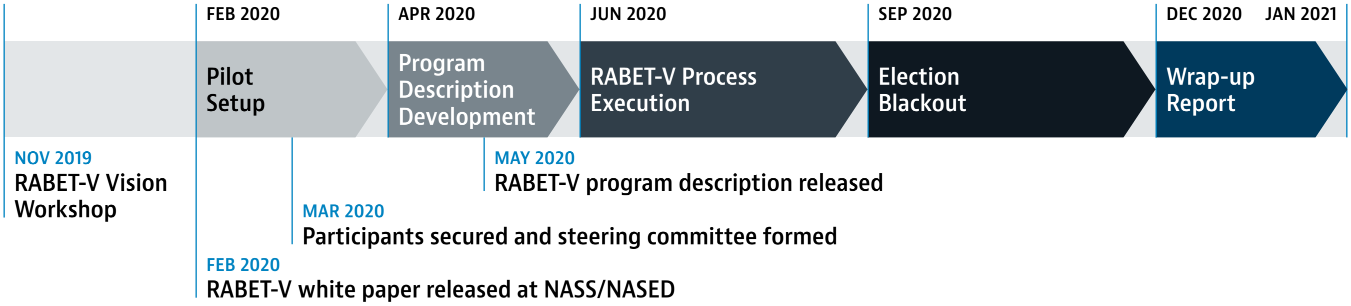
Beginning in early 2020, we launched our first pilot of RABET-V with two technology providers and three products: an electronic pollbook from each, and an election-night reporting system. As the RABET-V administrator, we created a steering committee for the pilot that consisted of representatives from the states of Indiana, Maryland, Ohio, Pennsylvania, Texas, and Wisconsin, as well as the Election Assistance Commission (EAC), Federal Voting Assistance Program (FVAP), National Association of State Election Directors (NASED), and the Cybersecurity and Infrastructure Security Agency (CISA).

We spent considerable time early in the pilot working with the providers and steering committee to develop the RABET-V Program Description. The Program Description is the step-by-step guide for how RABET-V works. Subsequently, we began evaluating the technology solutions.

We began with a review of the providers' documentation, and then interviewed company leadership and product and development personnel to conduct the process assessment, architecture review, and verification activities. As we progressed, we made updates to the Program Description. In early 2021, we provided reports to the technology providers that summarized their initial scores.

We are currently writing the final report and wanted to share our most important conclusions:

- **RABET-V is a viable process for non-voting election technology.** We successfully evaluated two electronic pollbooks and one election-night reporting solution using this new process.
- **We can evaluate architecture and use it to assess risk of changes.** We developed a rubric to measure architecture maturity and completed architecture reviews on three very different architectures.
- **We can evaluate software development processes and use the results to assess the likelihood of positive security outcomes.** We adapted the software assurance methodology from OWASP[1] and completed the process evaluation of two very different companies.
- **We can develop a testing matrix that prescribes different levels of testing based on the type of change, the architecture maturity score, and process maturity score.** We defined three testing tiers and


FEB 2020
APR 2020
JUN 2020
SEP 2020
DEC 2020
JAN 2021
Pilot Setup
Program Description Development
RABET-V Process Execution
Election Blackout
Wrap-up Report
NOV 2019
RABET-V Vision Workshop
MAY 2020
RABET-V program description released
MAR 2020
Participants secured and steering committee formed
FEB 2020
RABET-V white paper released at NASS/NASED

[1] https://owaspsamm.org/

created a testing matrix to determine which tier to use based on the combination of the three inputs and related risks.

- **Reevaluation of new product versions will be quicker for products with higher process and architecture maturity scores.** The testing matrix provides for lower effort testing methods for high maturity scores—without compromising security.
- **RABET-V can be run by a central administrator with various activities conducted by external specialists.** We acted as administrator and contracted with specialists to perform activities such as process assessments, threat modeling, architecture models, and testing.
- **RABET-V is compatible with multiple operational and economic models.** We developed a paper outlining the operational and economic models RABET-V could work with and validated it with the Steering Committee.

RABET-V Process

The RABET-V process consists of seven total activities, five of which are conditional activities that are scaled to meet the needs of the review. This scaling provides an adaptable, risk-based testing strategy informed by the product's architecture and the developer's processes and security claims. These factors, combined with the significance of the change itself, determine the overall testing strategy for each iteration.

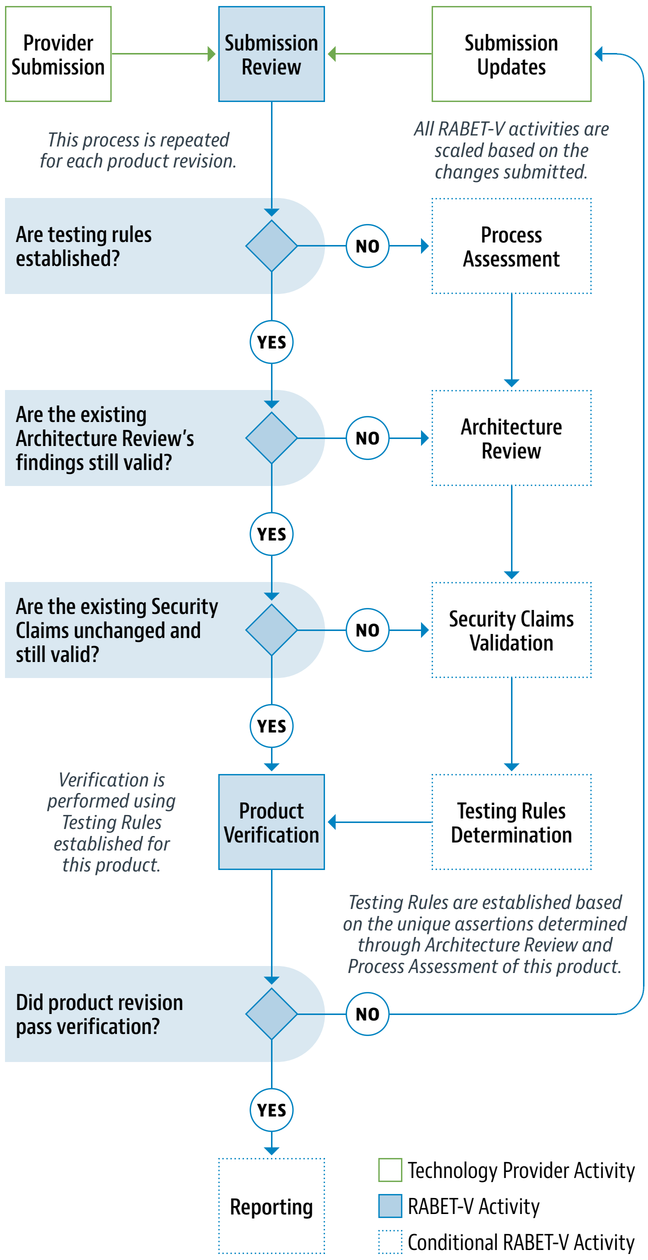
RABET-V presents a paradigm that balances multiple needs:

- A rigor of verification and testing that meets the needs of a critical application like those in the election environment
- Incentives for rapid development and deployment similar to those we see in highly innovative industries

The RABET-V program speeds up verification of software by deploying an iterative process for verifying technology products. First, when a new technology provider enters the RABET-V program, it goes through an organizational review and gets its software process maturity scored. Second, when a new product from that provider enters the RABET-V program, it goes through a full review of its architecture and design related to security. Third, the product is tested. The initial testing is a full test to set an initial baseline for the security controls implemented in the code and configuration.

When a product that has already been reviewed has a change, the technology provider can submit for an iteration review. In this case, the work done in the first round can significantly lower what needs to be done in an iteration review.

In the iteration review, if the technology provider's process review is sufficiently recent and the technology provider indicates that there have been no major changes to its process, this step can be skipped entirely. Alternatively, if they have made improvements in the process, they can submit for a streamlined review to update their process maturity score.


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

Likewise, if the architecture of the product and the security claims are unchanged in the new version, this step can also be skipped. If the changes are isolated, the updates can be isolated to those portions that changed and the relevant maturities updated.

Finally, the product is tested based on the established maturity scores. The stronger the maturity scores, the lower the burden of testing. For instance, if a technology provider has mature processes and a well-segmented architecture, a change to a single security service is unlikely to trigger changes to other services. In that case, the iteration testing can be scoped to only that service and related interconnections.

How RABET-V mitigates a SolarWinds-type attack on election technology

In December 2020, a leading cybersecurity firm announced that they had discovered a global intrusion campaign using a supply chain attack. This attack used the SolarWinds Orion business software to distribute malware that the cybersecurity firm named SUNBURST.[2] The consequences of this serious attack are not yet fully known, and likely won't be for some time.

While we currently believe there was limited or no impact on election infrastructure, this highly successful attack begs a question for all organizations: how do we prevent or mitigate such a sophisticated attack on our technology or on technology we use? There are many government and business leaders, along with the larger security community, searching for ways to answer this question. The RABET-V program that we have been piloting for the past year may provide some answers.

The RABET-V program is designed to verify the security of non-voting election technology in a rapid and effective way. This program, however, is not restricted to just non-voting election technology. Its tenets can be easily employed on other technologies and can be effective at preventing SolarWinds-type attacks. The table below summarizes some of the aspects of RABET-V and how those attributes could have prevented or mitigated parts of the SolarWinds attack and others like it.

Deeper Dive

In this section, we discuss some of the mitigations to a SolarWinds-type attack that are possible when verifying technology with RABET-V. No control, verification process, or set of mitigations can guarantee protection from all attacks. The SolarWinds attack was complex and advanced. Even the best organizations could be compromised by a sophisticated nation-state actor. Nonetheless,

RABET-V	Mitigating Effect
Provides a means of verification to technologies which have been traditionally difficult to verify quickly and reliably	Allows for more rapidly changing technologies to go through a verification process, increasing the likelihood that they may catch or mitigate attacks
Creates market-based incentives to encourage vendors to improve their internal development and technology security	Technology providers work to improve their published scores instead of just hitting minimum compliance standards
Designed as an adaptive and evolving framework to respond quickly to discoveries such as the SolarWinds attack	Allows for quick updates to account for newly-discovered vulnerabilities and new attack methods
Process assessments evaluate technology providers' internal software development processes and their mechanisms for evaluating and use of third-party components	Verifies whether the provider has proper procedural controls in place to prevent or mitigate insider threats and supply chain threats, and identifies changes to those processes over time
Evaluates all source code changes for their impact on security-relevant source code	Potential to catch an unauthorized source code change in a sensitive area of the code
Architecture review evaluates the quality of suppliers chosen by the technology provider	Providers select more reputable suppliers to achieve higher architecture scores
Evaluates the third-party software libraries used by the technology provider	Identifies the use of outdated, unpatched software libraries and requires providers to patch
Penetration testing evaluates network traffic, among other system attributes	Potential to spot unexpected and unauthorized network traffic

[2] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

the RABET-V approach can increase the likelihood of stopping attacks and decrease the impact of an attack if successful.

Motivating Continuous Improvement. Many programs (and most federal cybersecurity policy) have an approach to reviewing software that focuses on meeting a floor. There's little to no incentive to go above that, and the baseline is typically so complicated that there's no budget for innovating in security.

RABET-V presents a different incentive model. States can set minimums, but the primary mechanism is the publishing of maturity indexes that cover the provider's architecture, capability, and processes. These scores are known to the public, customers, and competitors, providing an incentive for the provider to be accountable and improve their scores. This approach will require the provider to consistently monitor their systems to prevent security regression and push for improvements.

Review Software Development Processes. RABET-V requires a process assessment of the technology provider that reviews their governance, design, implementation, verification, and operations processes.[3] Few other verifications take this deep look into the internal processes of an organization and treat them as leading indicators of security risk, even though security outcomes are clearly proportional to procedural controls. In fact, with the current evidence, SolarWinds' internal processes seem to have lacked the controls that would have caught the manipulation of their source code prior to deployment.

Promote Mature Architectures. The RABET-V architecture review process scores system architectures based on a prescriptive rubric that is biased toward modular architectures that isolate security-sensitive functions using reputable providers. Systems that score highly against the RABET-V architecture rubric:

- Can easily identify source code or configuration changes to their security functions
- Are less likely to have a security function be impacted by code injection in other areas of the system
- Are more likely to be using a third-party supplier that implements proper security controls
- Will have layers of defense to mitigate failures in other components

Source Code Awareness without Source Code Review. Source code review is a significant time and money investment for a verification process and doesn't typically have the benefits necessary to justify the cost. To address this, RABET-V uses a software analysis tool to perform change analysis on the source code modules.

The change analysis provides us visibility into what changed without detailed evaluation. We use this analysis to see if we need to perform another architecture review and to determine if the provider changed security related functionality. By flagging the security functions during the initial evaluation, the change analysis allows us to determine if the provider changed a security related component or added any new third-party dependencies.

The analysis has the added benefit of detecting new and unexpected changes for the provider and the evaluator. These are both benefits which, depending on the code injection like we saw with SolarWinds, may have detected the attack.

Conclusion

As mentioned earlier in this paper, no set of mitigations can guarantee protection from all attacks. The complexity of the SolarWinds attack was such that even the most sophisticated organizations could have fallen victim to it. That said, strong defensive practices increase the likelihood of preventing attacks and reducing the impact of successful attacks.

The RABET-V process provides incentives to implement best practices and to continually improve on them. It also allows for more rapid changes that can promote smart innovation with security in mind, promoting innovation without sacrificing security. Together, this presents a better opportunity to prevent and mitigate attacks.

The pilot administrator is currently seeking funding to continue the RABET-V pilot process and conduct a second pilot focused on additional electronic pollbooks and voter registration systems.

[3] The RABET-V process assessment is based on the Software Assurance Maturity Model (SAMM) from OWASP https://owaspsamm.org/.

About the Author

Aaron Wilson is the Sr. Director of Election Security at the Center for Internet Security (CIS), which administered the RABET-V pilot.

About CIS

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. 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 evolve these standards and provide products and services 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 rapidly changing cybersecurity needs of U.S. elections offices.

To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.