Engineering Trust

Using Rigorous Digital Engineering (RDE) to Build an End-to-End Verifiable Voting System Cryptographic Protocol

This issue paper details how a systems engineering approach — Rigorous Digital Engineering (RDE) — can bring formal methods, traceability, and a security-focused design to election technology development. It outlines how the Mobile Voting Project, in partnership with Free and Fair, had used this approach in developing a new end-to-end verifiable, open-source mobile voting protocol.

MOBILE VOTING

https://www.mobilevoting.org/

FREE & FAIR

https://freeandfair.us/

Why Use Rigorous Digital Engineering (RDE)

RDE is a development method that enforces traceability throughout the development and testing process by using formal methods including the development of common terminology definitions and a complete threat matrix/analysis performed before a single line of code is written. Other critical infrastructure systems have long implemented formal methods in their development processes and RDE is simply a natural progression of mission critical development in the elections industry.

The elections industry was recently designated as critical infrastructure by the US government and as such information sharing, security monitoring tooling, and other important critical infrastructure steps have been taken. But the core development methodologies of system development within the industry have lagged behind in this regard. RDE brings the development processes of election software in line with other critical infrastructure industries' formal development methods.

What is RDE?

Rigorous digital engineering (RDE) is a fundamentally different systems development approach that aims to eliminate the translation errors of the normal development process by introducing consistent rigor to software engineering at every step.

Domain Engineering: Creating a Shared Vocabulary
Often in the normal development process different teams use terms slightly differently or even within a single team definitions may be inconsistent. RDE attempts to create a shared vocabulary that is not ambiguous in any way and can always be referenced by all teams when approaching the tasks for each stage of development. This shared vocabulary is clearly presented, available at all stages and referenced where ever necessary to communicate clearly between teams and tasks.

Requirements Engineering: Defining System Laws
Equally as important as Domain Engineering is Requirements Engineering. Clearly defining every single thing the end system must 'do' in order to be considered complete MUST be defined early, revisited often for completeness, and understood by all teams involved in development. This is more than traditional stakeholder requirements gathering and should be informed by academic sources available, industry performance expectations and broader security requirements derived from other mission critical industries. All requirements MUST be traceable and all development and testing MUST trace back to one or more requirements. No work is performed that doesn't tie to these requirements.

Security Engineering: Withstanding Determined Adversaries
Other design and development practices are included in RDE but for elections one of the most important aspects of RDE is a focus on Security minded Engineering. A critical part of the RDE planning process is the creation of a detailed and complete threat analysis/matrix that covers every known attack vector or vulnerability in the planned system. Being transparent with known and potential threats does not make the system weaker, in fact, it helps demonstrate that the end system is taking into account all the possible security issues and has solved or mitigated for each in a documented and transparent manner.

Implementation in Election Technology and Future Development

RDE has been demonstrated on hundreds of software and hardware systems, and has been used on many projects to create secure, high-assurance software systems and ASICs. The kinds of engineering that have been incorporated into RDE include systems, software, firmware, hardware, safety, and security engineering.

A recent partnership has leveraged RDE to develop a new open-source mobile voting protocol. This protocol is the first known product of its type to use RDE as a baseline methodology for development. The solution represents a significant advancement in mobile voting technology, designed to reduce barriers to voting while maintaining the highest security standards. The hope of the two partnering organizations is that by demonstrating how RDE can be used within the elections industry, others involved in development and testing of critical infrastructure systems will be encouraged to pick up the practices for their own. Both organizations are committed to sharing all their knowledge about Rigorous Digital Engineering and all products created with it for the advantage of all within the industry.

Conclusion

This open-source mobile voting protocol provides a useful example of how RDE methods can be practically applied to an election technology context. Building on decades of research in election security and verifiable voting systems, the protocol was designed with a commitment to the transparency, rigor, and software assurance essential for critical infrastructure projects. The RDE methodology is highlighted within the project's public GitHub for all to follow, learn from and comment on.

The Mobile Voting Foundation and Free & Fair invite continued collaboration from security experts, researchers, and election officials to further validate and improve the system and the methodology involved.

Learn more about RDE and follow the project here:

https://github.com/FreeAndFair/MobileVotingCoreCryptography