US Voting Systems Security Working Paper: "Revisioning the U.S. Elections Process: Voting Security and Election Integrity" Georgia Institute of Technology[1]

Executive Summary
June 2019

Revisioning the U.S. Elections Process: A Framework for Voting Security and Election Integrity

Much has been written in the last few years about the security of U.S. voting systems. Perceptions of, and certainty in, the security of voting systems have significant impact on public confidence in electoral system integrity. This paper focuses on various dimensions of security in a comprehensive manner, while taking into consideration other key system objectives such as accessibility, usability and transparency. Ongoing public conversations about an ideal approach to protecting the integrity of elections have tended to lack a general reference model or even a commonly agreed upon set of security objectives. Basic concepts lack shared meanings and different players seem to have different standards to benchmark current systems.

This working paper 1) identifies key security policy challenges facing elections officials and 2) proposes comprehensive *General Model for Voting Security (GMVS)* as part of an *Independent Assessment Framework (IAF)* that could address many of these concerns. The GVMS is designed to be a comprehensive reference to evaluate election integrity. It outlines a set of requirements that are described as "not an end unto themselves, but they are requirements that must be met to protect the primary voting system requirements in an adversarial model." It basically outlines the aspects that a system must support in order to maximize its security. The proposed IAF takes into consideration the nature of the electoral process in the U.S., including various regulations, complexity of process, cost of certification, the slow pace of innovation and pressure on election officials.

Attending to and anticipating issues of security has become a challenging task for election officials — staying current on advances in IT and cybersecurity, developing lifecycle auditing and assessment plans before, during and after an election. The attached working paper proposes a new streamlined, standardized approach to assessing election security that lowers the burden on election administrators, while increasing the effectiveness of the evaluation process. This approach recognizes that, in evaluating the security of voting systems developed independently by private companies, the proprietary nature of these systems must be respected and honored.

Currently, the primary mechanisms that jurisdictions have to evaluate the security of these systems are to:

1. Ask developers of a system to provide a description of the security of their system, and assume that it is sufficient;
2. Ask developers of a system to document internal security testing, assessment, or evaluation;
3. Conduct their own assessment of the security of these voting systems, for example using inhouse expertise or external consultants.

The first two options are the least reliable as they depend on the sufficiency, robustness and objectivity of the voluntary disclosure from the system vendors which can be considered a conflict of

[1] This working paper was produced with support of Smartmatic Corporation. For more information, or to comment on this paper, contact Paul M.A. Baker, Ph.D., Georgia Institute of Technology, [paul.baker@gatech.edu].

interests. The third option is superior in terms of achieving the desired results, but from a practical point of view is cost-prohibitive to jurisdictions. It assumes that jurisdictions have the required time and internal expertise to adequately evaluate the material provided by the vendors.

The attached working paper proposes a reference model, part of a broader analytic framework on which system developers can draw on to generate consistent and independently verifiable security assessments. The framework includes:

1. An independently defined, end-to-end voting systems security model, **General Model for Voting Security, (GMVS)**, that serves as a benchmark to evaluate the security of a voting system. This ensures that the security evaluations fully represent a whole system, and not selected elements that could mislead election officials.

2. A full vulnerabilities assessment of the voting system, using a predetermined set of criteria, performed independently by a trusted third party.

3. Generation of an independent report based on the vulnerability assessment performed, shared with jurisdictions, with a summary report.

Given that jurisdictions have many security-related voting system options available to them, we believe that the General Model for Voting Security and associated Independent Assessment Framework offers jurisdictions a comprehensive, cost-effective, and time saving process for evaluating the complete system security. Further, this approach reduces barriers to actually understanding the complexities of current voting systems. A single, robust security assessment that provides apple to apple comparisons guarantees consistency across systems and jurisdictional requirements at reasonable cost.