Public Comment Bill Wiesner

REDACTED VERSION

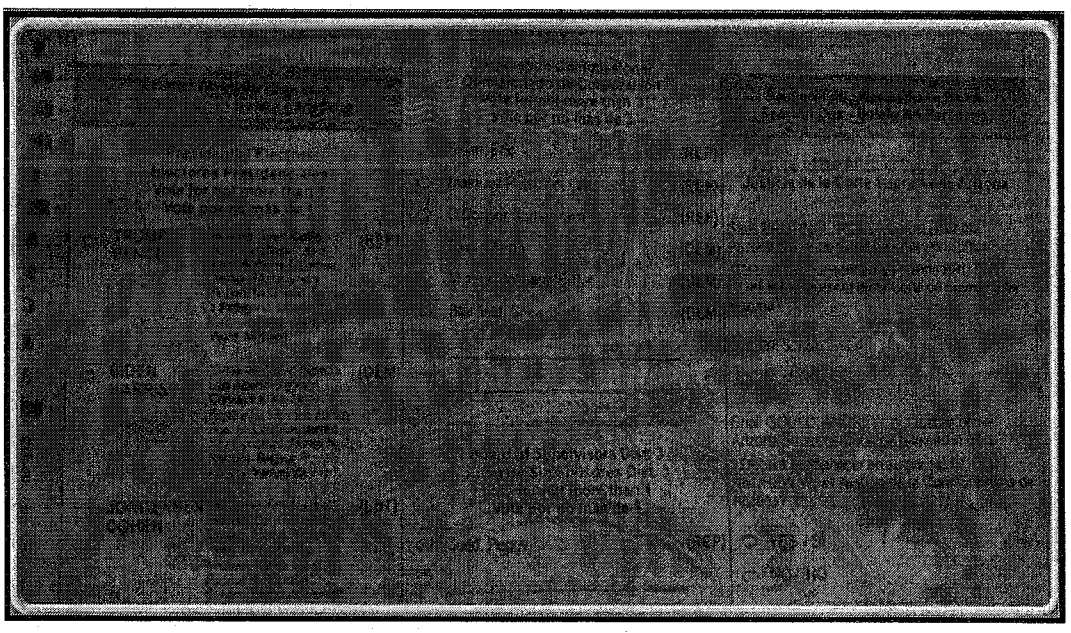
Security Analysis of Georgia's ImageCast X Ballot Marking Devices

Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al.
Curling v. Raffensperger, Civil Action No. 1:17-CV-2989-AT
U.S. District Court for the Northern District of Georgia, Atlanta Division

Prof. J. Alex Halderman, Ph.D.

With the assistance of Prof. Drew Springall, Ph.D.

July 1, 2021



Contents

REDACTED VERSION

1 Overview

In 2020, Georgia replaced its insecure, decades-old DRE voting machines with new ballot scanners and ballot marking devices (BMDs) manufactured by Dominion Voting Systems. Although the same BMDs are used for accessibility in parts of approximately 15 other states, Georgia is unique in using them statewide as the primary method of in-person voting [39]. This risky arrangement places potentially malicious computers between Georgia voters and their paper ballots. In contrast, in most of the United States, voters mark paper ballots directly by hand, and BMDs are reserved for those who need or request them [87]. Georgians who vote at a polling place generally have no choice but to use the BMDs.

All voting systems have cybersecurity risks. As the National Academies of Sciences, Engineering, and Medicine recently concluded "[t]here is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats" [58]. However, not all voting systems are equally vulnerable. Curling Plaintiffs contend that Georgia's universal-use BMD voting system is *so insecure* that it violates voters' constitutional rights.

To assist the Court in understanding the risks that the system creates, Curling Plaintiffs asked me to conduct a security analysis of the ImageCast X (ICX) BMD and associated equipment used in Georgia elections. Using an ICX provided by Fulton County, I played the role of an attacker and attempted to discover ways to compromise the system and change votes. I, along with my assistant, spent a total of approximately twelve person-weeks studying the machines, testing for vulnerabilities, and developing proof-of-concept attacks. Many of the attacks I successfully implemented could be effectuated by malicious actors with very limited time and access to the machines—as little as mere minutes. This report documents my findings and conclusions.[1]

1.1 Principal Findings

I show that the ICX suffers from critical vulnerabilities that can be exploited to subvert all of its security mechanisms, including: user authentication, data integrity protection, access control, privilege separation, audit logs, protective counters, hash validation, and external firmware validation. I demonstrate that these vulnerabilities provide multiple routes by which attackers can install malicious software on Georgia's BMDs, either with temporary physical access or remotely from election management systems (EMSs). I explain how such malware can alter voters' votes while subverting all of the procedural protections practiced by the State, including "logic and accuracy" testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs).

The most serious vulnerabilities I discovered include the following:

1. Attackers can alter the QR codes on printed ballots to modify the voters' selections. Critically, voters have no practical way to confirm that the QR codes

[1] I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this report and, if called to testify as a witness, I would testify under oath to these facts.

match their intent, but they are the only part of the ballot that the scanners count. I demonstrate how the QR codes can be modified by compromising the BMD printer (Section 5) or by installing malware on the BMD (Section 7).

2. The software update that Georgia installed in October 2020 left Georgia's BMDs in a state where anyone can install malware with only brief physical access to the machines. I show that this problem can potentially be exploited in the polling place even by non-technical insiders. (Section 8).

3. Attackers can forge or manipulate the smart cards that the ICX uses to authenticate technicians, poll workers, and voters. Without needing any secret information, I created a counterfeit technician card that can unlock any ICX in Georgia, allowing anyone with physical access to install malware (Section 6).

4. I demonstrate that attackers can extend arbitrary code with root (super-user) privileges by altering the election definition files that county workers copy to every BMD before each election. Attackers could exploit this to spread malware to all BMDs across a county or the entire state. (Section 9).

5. The ICX contains numerous unnecessary Android applications, including a Terminal Emulator that provides a "root shell" (a supervisory command interface that overrides access controls). An attacker can take the BMDs out of service simply by opening them in the on-screen Text Editor application. (Section 10).

6. In a given election, all BMDs and scanners in a county share the same set of cryptographic keys, which are used for authentication and to protect election results on scanner memory cards. An attacker with brief access to a single ICX or a single Poll Worker Card and PIN can obtain the county-wide keys.

7. The ImageCast Precinct (ICP) scanner stores ballot scans in the order they were cast. A dishonest election worker (like that emphasized by the Defendants and their expert Michael Shamos) with just brief access to the scanner's memory card could violate ballot secrecy and determine how individual voters voted (Section 11).

Proof-of-Concept Attacks In addition to discovering and validating the vulnerabilities described above, I developed a series of proof-of-concept attacks that illustrate how vulnerabilities in the ICX could be used to change the personal votes of individual Georgia voters. I am prepared to demonstrate:

1. An attack that uses malicious hardware hidden inside the BMD's printer to alter the votes on printed ballots. (Section 5).
2. Malware that runs on the BMD and alters votes while avoiding hash validation, firmware validation, and logic and accuracy testing. (Section 7).
3. An automated method of installing malware by briefly unplugging the printer cable and attaching a malicious USB device. (Section 8).
4. Vote-stealing malware that can be installed remotely from the EMS, by altering the BMD's ballot definition file. (Section 9).

Mitigation. Some of the critical vulnerabilities I discovered can be at least partially mitigated through changes to the ICX's software, and I encourage Dominion and the State of Georgia to move as quickly as possible to remedy them. However, merely patching these specific problems is unlikely to make the ICX substantially more secure. I did not have the resources to find *all* possible exploitable security bugs in the ICX software. Once I found one that satisfied a particular adversarial objective, I usually turned to investigating other aspects of the system. It is very likely that there are other, equally critical flaws in the ICX that are yet to be discovered. Fully defending it will require discovering and mitigating them all, but attackers would only have to find one.

1.2 Main Conclusions

On the basis of the technical findings described in this report, I reach the following conclusions:

- The ICX BMDs are not sufficiently secured against tactical compromise to withstand vote-altering attacks by bad actors who are likely to attack future elections in Georgia. Adversaries with the necessary sophistication and resources to carry out attacks like those I have shown to be possible include hostile foreign governments such as Russia—which has targeted Georgia's election system in the past [49]—and domestic political actors whose close associates have recently acquired access to the same Dominion equipment that Georgia uses through audits and litigation in other jurisdictions.
- The ICX BMDs can be compromised to the same extent and as or more easily than the AccuVote TS and TS-X DREs they replaced.[3] Both systems have similar weaknesses, including readily bypassed user authentication and software validation, and susceptibility to malware that spreads from a central point to machines throughout a jurisdiction. Yet with the BMD, these vulnerabilities tend to be even easier to exploit than on the DRE system, since the ICX uses more modern and modular technology that is simpler to investigate and modify.
- Despite the addition of a paper trail, ICX malware can still change individual votes and most election outcomes without detection. Election results are determined from ballot QR codes, which malware can modify, yet voters cannot check that the QR codes match their intent, nor does the state compare them to the human-readable ballot text. Although outcome-changing fraud conducted in this manner could be detected by a risk-limiting audit, Georgia requires a risk-limiting audit of only one contest every two years, so the vast majority of elections and contests have no such assurance. And even the

[2]Over the past six months, I have repeatedly offered (through Curling Plaintiffs' counsel) to meet with Dominion and share my findings, so that the company could begin developing software fixes where possible, but they have yet to take me up on this offer.

[3]I conducted similar analyses of the TS in 2006 [31] and the TS-X in 2007 [11].