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

Source: Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23

Background

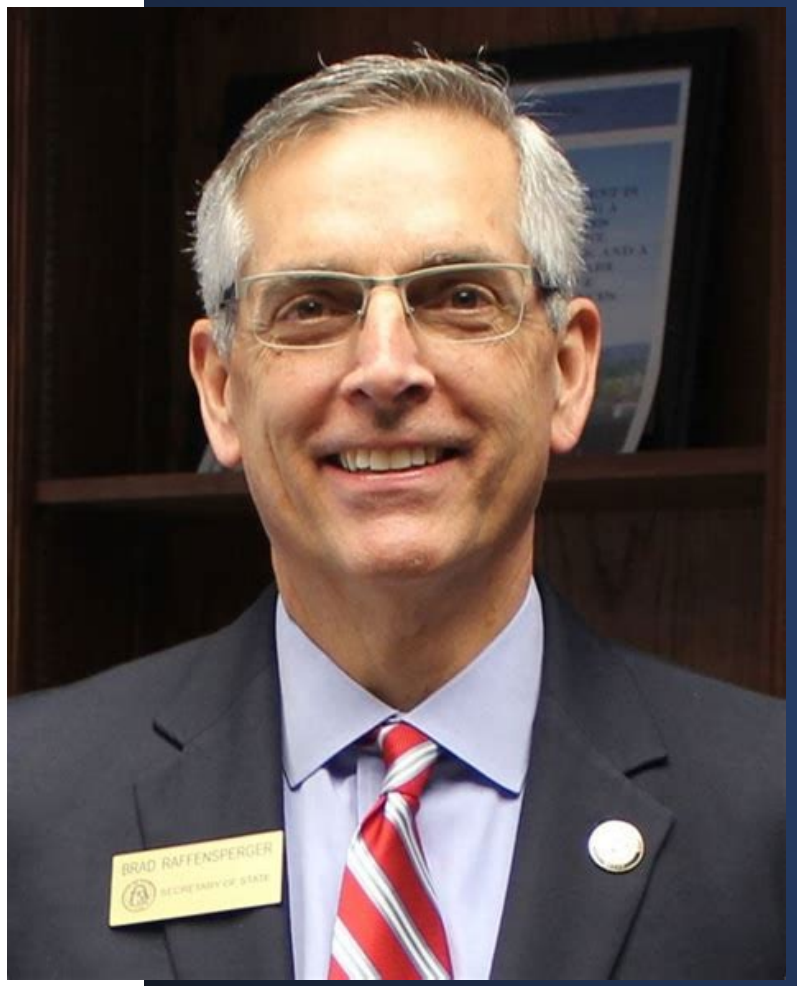
The “Halderman Report” is a 96-page document authored by Alex Halderman of Michigan State University focused on the vulnerabilities of the Dominion Voting System in Georgia. Halderman is:

- Professor of Computer Science & Engineering.
- Director, University of Michigan Center for Computer Security and Society
- Director, Michigan Computer Science & Engineering Systems Lab.

Brad Raffensperger

Mr. Raffenperger refutes the Halderman Report and offers “the MITRE Report” which is not signed by any computer scientist or anyone at all and Mr. Raffensperger’s background is:

- Civil Engineer educated at the University of Western Ontario, not Computer Science
- **He is not a computer scientist or programmer and has none on staff at the Sec. of State.**



Professor Halderman Concluded:

My technical findings leave Georgia voters with greatly diminished grounds to be confident that the votes they cast on the ICX BMD are secured, that their votes will be counted correctly, or that any future elections conducted using Georgia's universal-BMD system will be reasonably secure from attack and produce the correct results. No grand conspiracies would be necessary to commit large-scale fraud, but rather only moderate technical skills of the kind that attackers who are likely to target Georgia's elections already possess. Unfortunately, even if such an attack never comes, the fact that Georgia's BMDs are so vulnerable is all but certain to be exploited by partisan actors to suppress voter participation and cast doubt on the legitimacy of election results.

touchscreen

touchscreen

Haldeman Report Link

Prof. Halderman writes that the touchscreens can subvert ALL security mechanisms – not a few, some or many but ALL.

1.1 Principal Findings

touchscreen

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 acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs).

Haldeman Report Link

Prof. Halderman found that the scanners are using a Linux software version called “uCLinux” that was released in February 2007. Outdated, 16-year old software.

The ICP I tested runs a variant of the Linux operating system, μClinux version 20070130. μClinux is a Linux variant intended for use in embedded devices; version 20070130 was released in February 2007 [83] and is more than 14 years older than the most recent Linux version. A custom application named `cf200.sig` runs on top of μClinux and provides most of the scanner's functionality.

Haldeman Report Link

Professor Halderman found that ballot manipulation is a far greater risk for Georgians because our system relies on touchscreens for ALL IN PERSON voting.

Notably, both styles of ballot manipulation are far greater risks when BMDs are used for all in-person voters, as in Georgia, than when only a small fraction of voters use them, as in most other states. When few voters use BMDs, even changing *every* BMD ballot could only affect the outcome of contests with very narrow margins, and successful fraud would usually require cheating on such a large fraction of BMD ballots that it would likely be discovered. This makes the BMDs an unappealing target and reduces the risk that they will be attacked at

Haldeman Report Link

can be programmed to detect and circumvent LAT. For example, malware could be programmed to only cheat on the day of the election, or only during specific hours on that day. It could also be programmed to monitor how the machine was used and to only start cheating if the rate of voting, pattern of votes, number of corrected mistakes, and other characteristics matched the expected behavior of real voters. No practical method of pre-election or parallel testing can rule out malware-based fraud [80].

Professor Halderman found the touchscreens QR codes are not protected against “replay”: attacks so the scanners will accept a photocopy of a ballot or thousands of photocopies and the scanner will not stop the multiple scans.

5.2 Defeating QR Code Authentication

Issue: *ICX QR codes are not protected against “replay” attacks, so copies of valid QR codes will be accepted as genuine.*

As an authentication mechanism, the QR code contains a cryptographic message authentication code (MAC) computed using the HMAC-SHA256 algorithm.

Haldeman Report Link

Similarly, the attacker could remotely enable or disable the cheating, thereby defeating any pre-election testing. With wireless control, the attack device could be installed in the printer once and cheat in any subsequent election.

Adding hardware to the printer is only one of several ways that attackers could manipulate ballots cast using Georgia's ICX BMDs. An easier and more powerful mode of attack would be to modify the software in the ICX itself. When I demonstrated the printer attack prototype in September 2020, I testified that software-based attacks on the ICX were very likely achievable with further analysis. This has proven to be the case. In later sections of this report, I will explain how it is possible to construct vote-stealing malware that runs entirely in the ICX, and how attackers can infect ICXs with such malware remotely throughout entire counties or even the entire state.

Professor Halderman explained in detail how it is possible to create and install a vote-stealing virus that runs entirely on the touchscreen and that virus can infect all the touchscreens throughout the county and even the state. This is why we need old-fashioned paper ballots.

Despite this use of a MAC, attackers can manipulate ICX QR codes through several means to alter recorded votes or cast fraudulent votes. The ICX QR code design as used in Georgia has a serious weakness: the codes do not contain a serial number or other unique identifier, so, for a given ballot design, all QR codes that contain identical votes are indistinguishable, including having identical MACs. As a consequence, there is no mechanism for detecting *duplicate* QR codes. This enables two important attacks:

Copying Ballots A copy of a genuine ICX ballot will be indistinguishable from a second genuine ICX ballot with the same votes. In tests, the ICP accepted ballots copied using an office photocopier (see Section 11.1). This could allow a variety of ballot-box stuffing attacks.

Professor Halderman found that attackers can manipulate QR codes several ways to alter already recorded votes or to cast fraudulent votes. There are no serial numbers, no unique QR codes and a photocopied QR code is counted just like an authentic ballot which allows for ballot stuffing.

3.2 BMD Ballot Manipulation Attacks

The ICX, as used in Georgia, produces ballots like the one shown in Figure 2. They are printed on one or more sheets of letter-size paper. The ballot design uses a QR code (a kind of two-dimensional barcode) to represent the voter's selections in machine-readable form. Although the ballot also contains human-readable text

Dr. Halderman found that the Dominion scanners ignore the human readable text and only read the data in the QR Code.

that summarizes the selected choices for each contest, Dominion scanners ignore the ballot text and exclusively count the votes that are encoded in the QR code. Voters have no practical way to read the QR codes, so they cannot verify the representation of their vote that is counted.

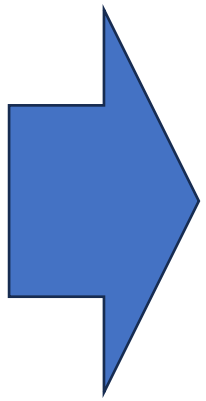
Reminder: ICX BMD is the touchscreen ballot marking device

Adding hardware to the printer is only one of several ways that attackers could manipulate ballots cast using Georgia's ICX BMDs. An easier and more powerful mode of attack would be to modify the software in the ICX itself. When I demonstrated the printer attack prototype in September 2020, I testified that software-based attacks on the ICX were very likely achievable with further analysis. This has proven to be the case. In later sections of this report, I will explain how it is possible to construct vote-stealing malware that runs entirely in the ICX, and how attackers can infect ICXs with such malware remotely throughout entire counties or even the entire state.

25

[10] In a realistic attack scenario, the attacker would likely choose to alter only a fraction of the ballots, so as to avoid drawing suspicion.

[11] My proof-of-concept implementation sometimes introduces a spurious delay of up to about 20 seconds before the ballot is printed. The most likely cause is a bug in the code. Having demonstrated the attack concept, I opted not to spend further resources debugging and removing the delay, and instead focused on attacking the ICX software.



There is no patch to fix this. Using a patch to fix a 2007 operating system is like taking the flat tires off a 1977 Pinto and putting on perfectly inflated BALD TIRES to drive in the rain. This is insane!

6.1 Extracting Election Secrets from Poll Worker Cards

Issue: *Anyone with access to a single Poll Worker Card and the corresponding PIN can easily extract secret keys and other values used for securing election data throughout the county.*

The ICX smart card protocol does not authenticate the device reading the card. As a result, anyone with the correct PIN can read the data on the card in a

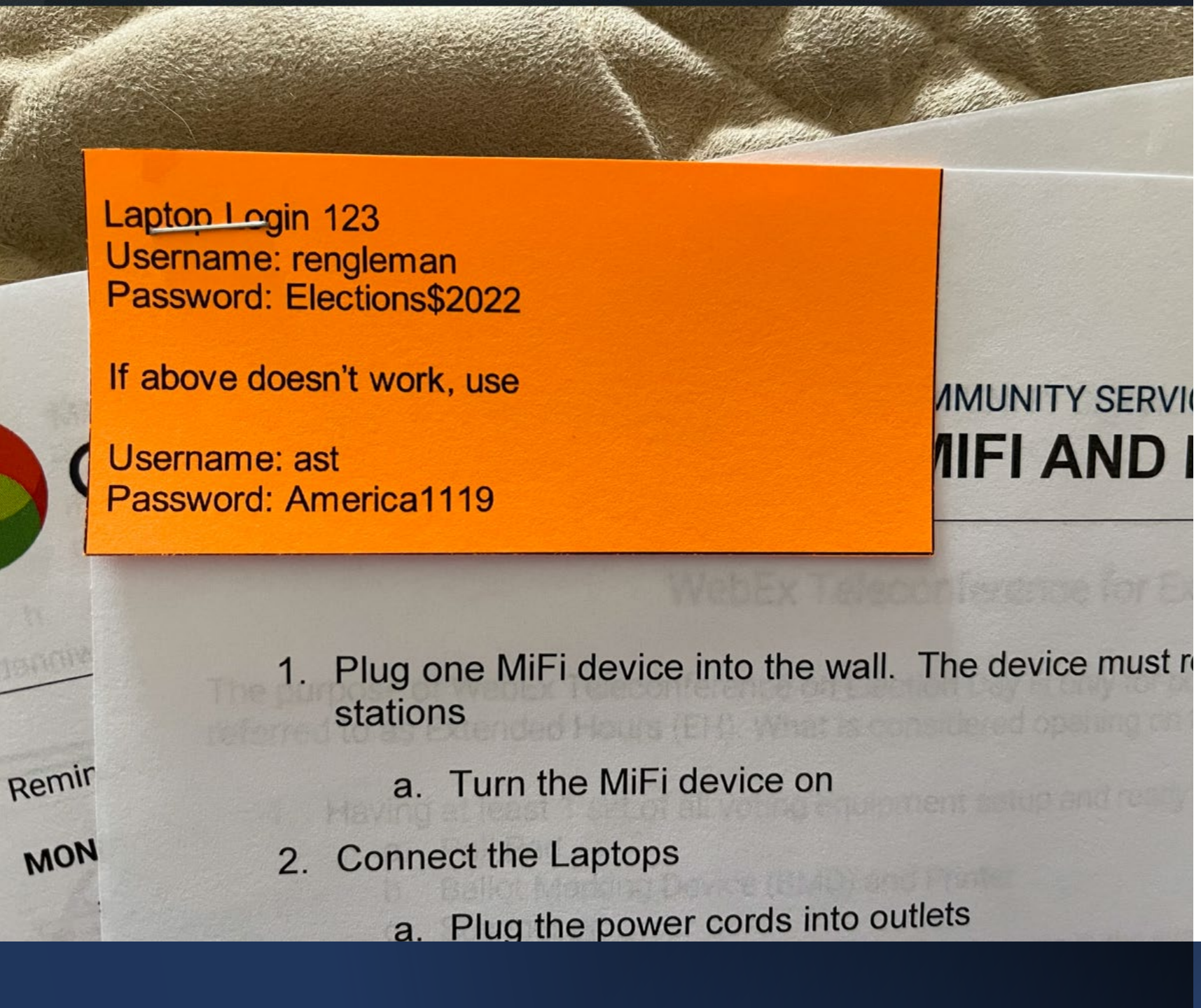
A single poll worker card can be used to compromise an entire county.

Source: Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23

Poll Worker Cards and PINs are distributed to every polling place and entrusted to thousands of volunteer poll workers across the state during every major election. It would be practically impossible to ensure that none of these cards could be temporarily accessed by a malicious party.

County election databases from the November 2020 and January 2021 elections shows that Georgia counties use the same cryptographic keys county-wide for each election. This means that if a single Poll Worker Card and PIN anywhere in a county is temporarily accessed by an attacker, the attacker can easily obtain the keys necessary to compromise election data throughout the county.

Source: Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23



How secure is a system with generic username and passwords?

Source: Gwinnett County

Figure 7: **Forged Technician Card.** Technician Cards can be forged without using any secret information. The self-created card can be used to unlock any touchscreen ICX in Georgia (and likely those in other jurisdictions) and install malicious software.

SERIOUSLY?

WE PAID HOW MUCH FOR THIS?

Source: Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23

file ID is.) To unlock the file, it accepts *any* password, so the user can enter any PIN. The card then returns a file that is *completely empty*, with every record consisting of zeroes. Remarkably, the ICX accepts the card as if it were a genuine Technician Card.

touchscreen

ICX Technician Cards are not restricted to a particular election or a particular jurisdiction. Consequently, the forged Technician Cards I created will work in any ICX across the State of Georgia, and likely in any other jurisdiction that uses a compatible version of the machine.

touchscreen

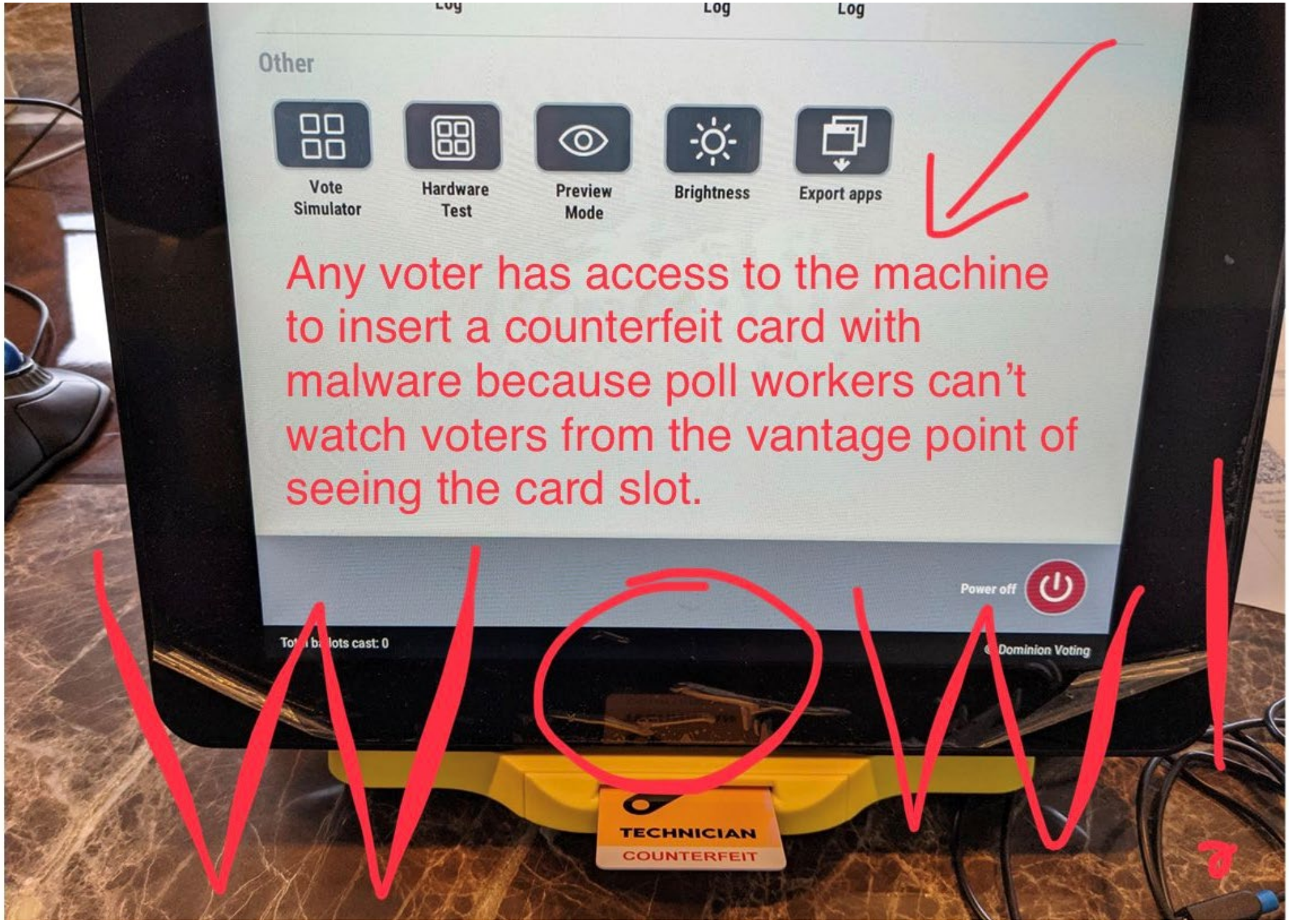
After forging a Technician Card, an attacker with physical access to a BMD can exit the ICX application and access the underlying Android operating system. With this access, the attacker can arbitrarily change the BMD's configuration, alter audit logs, or install malicious software.

Source: Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23

Poll managers in Georgia know that all voters in their precincts have access to the touchscreen slot because nobody is allowed behind a voter when they are voting. Any voter could insert a smart card without detection.

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).

Haldeman Report Link

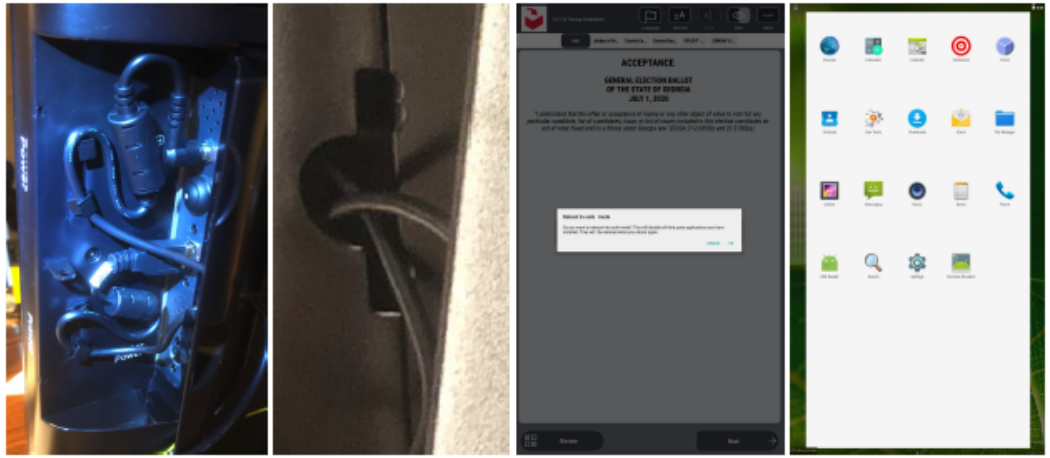

Log
Log
Log
Other
Vote Simulator
Hardware Test
Preview Mode
Brightness
Export apps
Any voter has access to the machine to insert a counterfeit card with malware because poll workers can't watch voters from the vantage point of seeing the card slot.
Power off
Dominion Voting
TECHNICIAN
COUNTERFEIT
WOW!

8.7 Local Malware Installation via Android Safe Mode

Issue: *A local user can reboot the ICX into "Safe Mode", allowing full control of the Android operating system.*

A third method for installing malware is to exploit a publicly known security flaw in the ICX. According to a Dominion customer advisory dated January 2020, "[i]f the mechanical power button (behind the ICX door) is pressed a power down option is presented. At this point, if the power down screen button is pressed and held, the 'safe mode' option is presented" [22].

I tested this behavior on the ICX. As shown in Figure 13, holding the power button and selecting "Reboot to safe mode" will cause the BMD to restart with the standard Android Launcher available, providing unrestricted control of the device, including access to the Android Settings, File Manager, and Terminal Emulator apps and the ability to install or remove software.



Any non-technical user can press and hold the power button to open the "safe-mode" menu which allows full control of the operating system.

Layman's Translation:

A third method for installing malware is to exploit a publicly known security flaw in the touchscreen device. According to a Dominion customer advisory dated January 2020, "If the mechanical power button behind the touchscreen door is pressed, a power down option is presented. At this point, if the power down screen button is pressed and held, the 'safe mode' option is presented" .

Professor Halderman tested this behavior on the touchscreen and the machine allowed him to Reboot to safe mode, providing unrestricted control of the device

Source: Case 1:17-cv-02989-AT Document 1681 Filed 06/14/23