What is the "Opportunity to Mark" Design Flaw?

Kevin Skoglund, Citizens for Better Elections

Prof. Andrew Appel from Princeton University discovered a voting machine flaw in October 2018 and wrote about it on his blog.

https://freedom-to-tinker.com/2018/10/16/design-flaw-in-dominion-imagecast-evolution-voting-machine
https://freedom-to-tinker.com/2018/10/22/an-unverifiability-principle-for-voting-machines

Summary of the flaw: After a paper ballot is verified and cast by the voter, the paper ballot travels past the print head that marked the paper ballot again before it is tabulated. The BMD is physically capable of printing additional marks on the ballot after verification and before tabulation. The printing could be caused by hacking or by malfunction.

Three voting systems have this flaw:
- Dominion ImageCast Evolution
- ES&S ExpressVote XL
- ES&S ExpressVote (when configured as a tabulator)

The flaw is similar to hand-counting ballots which have been marked by pen while the people doing the counting hold pens in their hands that are exactly like the pens used by voters to mark the ballots. The counters could, either accidentally or intentionally, mark ballots before or after counting them. We could no longer have confidence that each ballot was the same as when the voter verified it. It is common sense that a ballot must be protected after being cast to prevent alteration.

This is a serious flaw that can change election results or affect the auditability of those results to prove they are correct. Ballots should not pass any marking device again before tabulation to ensure that they are counted as cast. Ballots should not pass any marking device again, before or after tabulation, to ensure they can be reliable evidence for audits.

A ballot could be altered by a hacked or malfunctioning voting machine to:
a. invalidate a vote by overvoting in a contest
b. add a preferred vote anytime a ballot contains an undervote
c. alter a barcode to give it new meaning
d. deface a mark or barcode to prevent tabulation
e. add an additional barcode if space allowed
f. deface a human-readable vote summary to prevent auditing
g. deface an entire ballot to prevent tabulation or auditing

If this serious flaw was known in October 2018, why are we hearing about it now?

The flaw was initially identified in the Dominion ImageCast Evolution (ICE) but its effect was limited. The ICE was a new product which was tied up in patent-infringement litigation for many months. It was not certified for use in most states and was not being widely offered or purchased.

It was suspected that the ES&S ExpressVote XL and ES&S ExpressVote (configured as a tabulator) had the same design flaw, but it was only confirmed recently.

The issue received more attention when, on March 7, 2019, the New York State Board of Elections Co-Chair, Douglas Kellner, sent a memo to the full board recommending that the Dominion ImageCast Evolution be re-examined for certification because of this design flaw. [https://www.scribd.com/document/401448810/190307-Kellner-Memo-Dominion-ICE-Copy]

Does this design flaw affect any Pennsylvania voting systems?

Yes. The ES&S ExpressVote XL and ExpressVote configured as a tabulator are certified for use in Pennsylvania. The Dominion ImageCast Evolution has not been certified for use in Pennsylvania.

Philadelphia and Northampton Counties have begun the process of purchasing the ES&S ExpressVote XL.

Other Pennsylvania counties (including Beaver, Berks, Centre, Greene, Lawrence, and Lehigh) are purchasing the ES&S ExpressVote; however, news reports indicate they will be configured as ballot marking devices only and use separate optical-scanners without a printer or an "opportunity to mark" to tabulate them.

Is this the same as the "permission to cheat" vulnerability?

No. That was a separate vulnerability described by Prof. Appel in September 2018. [https://freedom-to-tinker.com/2018/09/14/serious-design-flaw-in-ess-expressvote-touchscreen-permission-to-cheat/] It just happens to be present in the same three voting systems. The two problems are not linked. The AutoCast feature ("permission to cheat") has been disallowed in the Pennsylvania certification of these systems.