A Plea for Disaster Avoidance
- or -
The Law That Will Save America

By: Matthew Grayson

Laws are coming that will change how American's vote nationwide. So far it's an unremarkable technology that will allow everyone to vote from home, from their own computers. It's coming, and I will be as brief as I can on how it will work. E-Voting is a voting system that uses the internet to process votes for public office. Reference material on this subject matter and information for contacting your state officials is at the end of this document.

The points of this are simple. A federal law has to be created now to stop E-Voting from being adopted as standard practice for public office. E-Voting opens the doors to massive corruption for elections nationwide. This brief explains how internet voting will be pushed as a good thing, and how it will fail.

Right now, E-Voting software is being developed for every American across the nation. Most people aren't aware of the changes taking place. This software will make it possible to vote from home, never leaving your computer or going to a polling booth. It will have the authentication characteristics necessary to hold up under intermediate scrutiny from the front end of the system. The back end of the system will be in the sole hands of administrators. There will be no usable physical evidence that voting has taken place. Only a digital authentication trail will be available for audit. This new voting system will soon be in place and it will gain traction quickly. You will either use it, or you won't vote at all.

Creating a foundation for E-Voting

Supporting laws will be drafted that provide for this effort. States will be required to use the system for elections. E-Votes cast will be collected over the internet into a central server and results will be counted, and probably revealed in real time. Registration for voting will be unsupervised and by the voter (end-user) alone. There will be little or no oversight on who is allowed to vote in the United States.

Registration for E-Voting is another issue beyond the scope of this explanation. However, it's possible that people will be allowed to take a digital picture of their photo ID, and submit it to the voting system to be authenticated. Face-pattern templates may be used to verify the parameters of photographs that are evaluated as legitimate or not. The same software tools used for facial recognition will determine authenticity of voters compared against whatever ID they produce. Accountability will be declared by proponents of the system, regardless the innumerable flaws.

How votes will be gathered and counted

The outcome of elections will be in the hands of technical experts that control the servers collecting the votes. In the interim (of network communications between the voter and tabulation) will be so vague that any sort of data manipulation may happen and never be traced out. *Real time data of incoming votes can be melded with any desired aggregate to reveal any pre-chosen winner without raising suspicions over the* *eventuality of the process*. It is a simple matter of basic addition and balancing over a known time base. This will completely destroy individual vote reliability across all domains of public office. The lack of a physical audit trail obliterates all meaningful accountability measures.

How E-Voting will be justified

But the argument will be this… *using crypto-authenticated accounts and trusted platform module technology ensures voter safety and election integrity.* And that is flat out not the case. E-Voting systems will inevitably lead to complete fraud across the spectrum without any recourse for the voters. There won't be any way to perform a realistic audit of the votes should the issue arise.

How can this be something that's happening and we aren't aware of it? Well, you are. Until recently Microsoft had noted that Windows 10 would be their last operating system. From there on out it would be a matter of ongoing updates.

Building the software voting platform

Less than a year after the massive debacle of the 2020 election, Microsoft has announced that instead they're going to come out with a new version of Windows. You have no doubt seen or read about the new Windows 11 and it's already shipping on computers for the 2021 holidays (officially launched October 5, 2021). This interesting move comes on the heels of the Dominion voting system being spotlighted for fraud. So what's remarkable about the new version of Windows that anyone would probably overlook, but at the same time will enable home based E-Voting?

Windows 11 makes another move to keep the end user from using a local account to the computer. Instead, every effort is made to maneuver all users to login to their *free* Microsoft account to use the operating system. Most people may see this as a blessing, since their cloud-based account will preserve their identity, store data, and backup critical information. In the case of new installations of Windows 11, there is no choice otherwise. But this is just one more step in keeping computers and the vast user base continually connected to the internet.

The Trusted Platform Module

However, there is something called a Trusted Platform Module (ISO/IEC 11889) that creates the international standard for a secure cryptoprocessor. Windows 11 now has these modules as a system requirement for the OS to run. Note that TPM has been around for about twenty years and ISO standardized since 2009. The most recent update to TPM was version 2.0 in November of 2019. It was originally conceived by the Trusted Computing Group (TPG) and has gradually insinuated itself into coexistence with operating systems and applications. So the hardware isn't new. Having a new operating system require it isn't so remarkable on its own either. But not all computers in the world have these chips in them. *The Microsoft Windows Operating System is the most concentrated deployment of software in the nation and worldwide*. The fastest way to ensure that every home winds up with a TPM chip is to make it a requirement for the new Windows 11 Operating System. So already, all of the existing hardware that doesn't have a TPM module was forced into obsolescence and all the new computers will be certain to have one by default. It's a quick matter of time for this new hardware base to be reliably installed across the country. And it's also important to note this is just another stepping stone, and that any computer equipped with a TPM module running any operating system will be a candidate for E-Voting. However, the remarkable prevalence of Microsoft's distribution density in the United States allows their Operating System to enforce massive cooperation across the hardware industry.

Big deal right? So what if Windows 11 has access to a cryptoprocessor? It's a very big deal. Step one to make it possible for E-Voting nationwide (for all public office) is to ensure all homes have their own voting booth. For this to happen, there must be a way to authenticate the machine's unquestionable and unique identity that cannot be hacked by software, firmware, or duplicated in any way. That is what the Trusted Platform Module (TPM) will do for the operating system.

A technical explanation, then a simple one

Voting servers will be established for the home computers to use for logging in. A handshake between the home computer and server will exchange the cryptographic information necessary to prove the system is secure. It will be argued that this is scientifically sound and extremely reliable. And that's certainly true for the sake of the connection. It will also be true that the account of the voter will be secured so that more than one person can vote on the same computer just like more than one person uses a physical voting booth today. For all intents and purposes this will appear to be reasonable. Votes will be sent from the home computer to a vote collection server on the internet. The movement of the data from voter to server will be safe and secure, delivering the intended votes as desired. Anyone observing both ends of the voting transaction will be content with the process. Keep in mind that votes take place over a domain of time, from the start of voting until the time is up. It's during this period a certain amount of traffic is expected as votes come in slowly, then fast, and then dwindle to the remaining to be counted. That curve of activity during the process can and likely will be seen in real time. So how does this fail if we can see what‘s happening?

The vote itself can be accounted for. You will be able to login to your voting account to double check what the server has on file for the vote(s) you placed. To that end, the server will have a total count of all votes for everyone for any given election. However, you will not be able to prove that your vote was ever included in the final outcome. Tabulation is done on the server by software. Except for the existence of the TPM chip, there is zero physical evidence that you ever did anything at all. The vote is purely digital information. It can be shuffled, sorted, ignored, deleted, or altered on the server side in a completely different database from the one the voter has access to when they login to see their votes.

The simple explanation

In essence, it's like keeping two sets of financial books. One book reflects reality. Another one altogether has the desired appearance of being accurate. The one the voter can see reflects their authenticated vote and is correct according to the server's response to query. The other book, or database, is the adjusted outcome that reveals the winner of the election(s) as seen fit by the administrator(s) of the server. So when the voter asks to see their records they see reality. When the votes are tabulated it's up to the administrator to use actual data or invented data.

So there is no way to audit the real votes as they are reported in the final results. The incoming data-stream of votes to the server could effectively go into memory oblivion as long as the aggregate of votes are preserved. The server only has to coordinate the actual number of votes collected incidental to what the votes truly indicate for the system to produce any falsified outcome. In the end, there is no way to reverse audit what actually happened during tabulation without the traditional paper trail of ballots.

A complete lack of reliable auditing

The primary failing for E-Voting is a lack a physical media in two parts. Physical media is something that can be touched by hand, handled back and forth, and examined with human eyes. Physical media can be easily comprehended when it fails by human inspection – a missing signature, tear or crease, lack of seal, smudge, and so on. *Physical media has permanence in the real world compared to digital data that can be obliterated without a trace*. Even if ballots were burned, there would be trace evidence of their existence. Digital platforms are highly susceptible even under the most rigid constraints. Consider the SolarWinds cyberattack disclosed December 2020 as just one example. Digital-only votes are as good as the paper they are recorded on - which is none.

Secondly is the lack of human personnel during the entire voting process. Polling Places will be effectively eliminated. As a result there will be no presence of Poll Watchers. Direct human involvement during the election is essential for accountability. If E-Voting is implemented, all reasonable oversight will be lost through the elimination of actual people watching over the entire process. Without the supervision of the American people themselves, the votes have no credibility.

E-Voting is the downfall of public office in the United States.

E-Voting must be stopped now with federal laws

A federal law must be put into place now, before any other law can be conjured that will support the ideals of E-Voting. This new law must make it illegal to use home computers or any other computer system that is not central to a specified public voting location to be used for the appointment of any public office. The law must clarify that the existing layers of traceability and chain of custody over the physical assets of paper materials such as ballots be maintained as a security contingency against fraud. It is critical to regulate and enforce voting systems to domains of implementation that rely on physical assets exclusively and to illegalize any sort of E-Voting system altogether. This has to be done for every state in the United States to have an effective measure of preventing fraud and corruption.

Conclusion

The steps of development for this to take place have been happening over many years. The gradual process of integration and deployment has gone unrecognized by most. However, the sudden change of Microsoft's former stance and release of a new operating system has brought the fundamentals into focus. All the elements necessary to deploy at-home E-Voting has come into immediate delivery. The only thing that's lacking are laws to enforce it. To that end, federal laws have to be addressed *now* to stop it before it gets started.

Thank you for your time and consideration.

Please send a copy of this .PDF file to as many people as you can and most certainly your elected officials. You can find who represents you using this website:

https://www.congress.gov/members/find-your-member

Click on the member(s) from the search and you will see an additional website specific to each member of the House of Representatives or Senate for your area. Click to proceed to that member's personal website for contact information.

You can find a copy of this document for reading, printing, forwarding, and sharing - download from:

https://www.avld.us/

REFERENCES

Microsoft Windows 11 System Requirements that list the TPM module described here can be found on the Microsoft website here:

https://www.microsoft.com/en-us/windows/windows-11-specifications

A June 29th 2015 Microsoft Security post titled "Governments recognize the importance of TPM 2.0 through ISO adoption" outlines the ideology of worldwide adoption of the Trusted Platform Module. You can read that article here:

https://www.microsoft.com/security/blog/2015/06/29/governments-recognize-the-importance-of-tpm-2-0-through-iso-adoption/

A variety of articles on this subject can be searched out, but the most impressive was a Staffordshire University dissertation published in July of 2010 by Mervat Adib Bamiah, associated with The International Research Academy of Science, Engineering and Advanced Technologies (IRASEAT).

A copy of the research paper can be found on the researchgate.net website where you can download the .PDF file. That link is here:

https://www.researchgate.net/publication/275270868_A_Trustable_Electronic_Government_Voting_Management_Framework_Using_Trusted_Platform_Module_TPM

You can also download Mervat Adib Bamiah's dissertation from:

https://www.avld.us/