Appendix D Passwords

We analyzed the access control mechanisms in the iVotronic software to determine whether they ensure that only authorized users are able to invoke sensitive functions on the machines. The iVotronic uses password protection to control access to sensitive functions. Therefore, we analyzed all uses of passwords in the iVotronic.

We found several passwords, used for different purposes:

- The Service Menu password is used to control access to the Service Menu, which provides functions that would ordinarily only be needed in the county warehouse. The Service Menu is not normally used by poll workers.
- The ECA password controls access to the Elections Central Administration menu. This menu provides additional functionality over and beyond the Service menu. The ECA menu is only accessible from the Service menu; therefore, reaching the ECA menu requires knowledge of both the Service password and the ECA password.
- The Clear and Test password is used to control access to the clear and test operation. The clear and test operation erases all votes stored on the iVotronic machine and prepares it for use in the next election. Because this operation can irreversibly delete votes, this is a sensitive function that must be protected from unauthorized individuals.
- The Election Qualification password is used to prepare a machine for a new election.
- The Upload Firmware password is used to control the ability to upgrade the executable software resident on the iVotronic's internal flash memory. This is an extremely sensitive operation, because it allows replacing the iVotronic's software. If this were invoked by a malicious individual, they could use it to install malicious software on the iVotronic machine or to infect it with a virus. This operation is available as a menu option in the Service menu. Therefore, invoking this operation requires knowledge of both the Service password and the Upload Firmware password.
- The Override password is used to control certain exceptional conditions that should not normally arise. For instance, if the user tries to close the polls on an iVotronic machine before the official time when the election is due to end, the machine requires the user to enter an override password before proceeding.
- The modem password is used by the iVotronic machine to transmit results back to the Unity Data Acquisition Manager (DAM) system at the county headquarters. When the iVotronic machine connects to the Unity server over the telephone, it first sends the modem password over the phone. While we do not have access to the Unity server source code to check how the Unity server uses this password, it would be logical to presume that the Unity server checks that the proper password has been sent before allowing the connection to continue. The modem password does not need to be known by any human.

Typically, the override password would be the only password divulged to poll workers; the other passwords would not be revealed to poll workers, and would be told only to county election workers.

Next, we analyze password security strength to determine if they can be guessed by an ill-intentioned individual. The modem password can be set at the Unity server when the election is configured. It is included in the election definition file. It is listed in the clear in the election definition file found on every PEB and, eventually, on every iVotronic machine. It is the same for

all iVotronic machines within a county. If it is not set, there is a default value hard-coded into the source code; this default is the same for all iVotronic machines across the nation. It is up to election officials to choose this password in a way that ensures it is unguessable, to change this password frequently (e.g., after every election), and to control who knows the password. Those are operational questions that are beyond the scope of a source code review.

Like the modem password, the override password can also be set at the Unity server when the election is configured. It too is included in the clear in the election definition file found on every PEB, and it is the same for all iVotronic machines within a county. It is selected and managed by election officials, so the management of this password is beyond the scope of a source code review.

Each of the other passwords mentioned above is fixed and hard-coded into the source code. They are the same for all iVotronic machines in the country, and likely to be known to every election official who manages elections on an iVotronic machine. They can never be changed, without changing the firmware on the iVotronic machine. This represents poor practice.

The Service Menu password, Clear and Test password, ECA password, and Upload Firmware password are three-letter case-insensitive passwords. Each one is chosen to be mnemonic and easy to remember. The problem is they are also likely to be fairly easy to guess. They follow a memorable pattern. Someone who knows one of these passwords can probably guess what the other ones are without too much difficulty. These passwords provide very little security.

The Election Qualification password is a five-letter case-insensitive password that is chosen to be easily memorable. It does not follow the same pattern as the other passwords.

The weakness of the Upload Firmware and Service passwords are of primary concern, because someone who knows those two passwords can replace the software on the iVotronic with malicious software that switches votes from one candidate to another, that turns valid votes into undervotes or deletes them entirely, that infects the machine with a virus, or that otherwise compromises the integrity of the election. These functions should be better protected.

Our judgment is that the password mechanisms on the iVotronic are poorly conceived and poorly implemented. The consequence is that the passwords by themselves do not do a good job of preventing unauthorized individuals from accessing critical system functions.

Finally, these passwords can all be bypassed using a special type of PEB, called a Factory Test PEB. When a PEB is inserted, the iVotronic machine queries the PEB to ask it what kind of PEB it is, and the PEB returns a single byte indicating what type of PEB it is. A Factory Test PEB identifies itself by returning a special single-byte value. This special value is hard-coded into the iVotronic code. Anyone who knows the special single-byte value, has access to a PEB and is able to program the PEB could construct a PEB that identifies itself as a Factory Test PEB. When a Factory Test PEB is present, all password checks are bypassed: in places where the user would normally need to enter a password, the password check is bypassed, the machine functions as though the correct password had been entered, and a log entry is appended to the event log as though the user entered the correct password. This undocumented backdoor poses a risk of unauthorized access to critical system functions, because it provides a way that a malicious individual could bypass the password checks by tampering with a PEB.