Voting Machine Forensic Analysis

Victor Ongkowijaya, Stephen Nurushev
EECS 498-009 - Election Cybersecurity, University of Michigan

Introduction

Used voting machines can be easily found on online shopping platforms today. The sale of these machines, which served in actual elections, raises many security questions: What measures are in place to protect confidential election data stored in memory? To what extent can attackers recover and overcome such measures? How can attackers utilize this information to jeopardize future election processes? Our study aims to utilize forensic analysis to answer these questions and explore the possible dangers of exposing used voting machines to the general public. We have acquired two used voting machines, the WinVote AVS and the iVotronic ES&S, both of which were widely used in multiple states and elections. Although past research has proven these models to be very insecure, to our knowledge not much work has been done to analyze used machines available online -- a relatively new attack vector. Unlike much of the past work in this field, we do not utilize special resources such as voting software source code, binaries, or anything not openly available online, much like potential attackers. We present a ground up analysis of these machines from exterior inspection to hardware disassembly and software live/dead analysis. In the process, we also aim to provide a methodology of forensic analysis specifically for voting machines, which would be useful not only to assess security risks but also to improve future response to potential security breaches.

Figure 1. A popular voting machine model sold on eBay for under $100. As many as 89 used machines have already been sold.

Background

Due to its open-endedness, forensic analysis greatly benefits from any background knowledge. Knowing what to expect and what to look for reduces the sense of “trying to find a needle in a haystack” that accompanies exploring a large and unknown system. This is especially important for voting machines, which have a narrow range of usage, purpose, and context, which would aid us in performing effective analysis. In this section, we present the machines we have selected to study as well as relevant background information.

1. Machine Selection

We begin by selecting the voting machine models to study. Some machines available to us are the WinVote by Advanced Voting Solutions, the iVotronic by Election Systems and Security, the Accuvote TSx/OS by Diebold, and the Optech IIIP Eagle by Business Records Corporation. We chose to work with the WinVote and the iVotronic due to a variety of factors. Both machines utilize Windows, an operating system we are familiar with, and both were widely used in recent elections. The greatest obstacle we found was that other machines utilize proprietary file systems and file formats, which would require additional specialized tools and techniques outside the scope of our study.

2. WinVote

The WinVote is a touchscreen Direct Recording Electronic (DRE) voting machine widely used in Virginia, but also licensed in Pennsylvania and Mississippi. It was first produced in 2003 by Advanced Voting Solutions and officially discontinued beginning with the 2016 elections. Widely dubbed as "America's worst voting machine," the WinVote was shown by many independent research groups to be extremely vulnerable. It runs Windows XP Embedded with no service packs, as well as an always-on wireless 802.11b LAN to communicate with other machines in the same voting precinct using WEP, the insecure precursor to WPA and WPA2. Past work has found that passwords across all machines are hard coded and cannot be changed. For example, its WEP key is "abcde", its admin password is "admin", and its Microsoft Access database password is "shoup". Together, these vulnerabilities make the WinVote not much more than an ordinary file server, which can be trivially man-in-the-middled when communicating with other machines in the precinct, and can have its data easily extracted by anyone in range of the wireless LAN. The machine we analyzed can be seen in Figure 2.

3. iVotronic

The iVotronic is another touchscreen DRE voting machine still in use from 2004 in Arkansas, Colorado, Kansas, Missouri, North Carolina, Ohio, Virginia, and Wisconsin. Despite past research showing that these machines are susceptible to a variety of attacks, its usage remains widespread. It runs Windows XP and operates very closely with the Personal Electronic Ballot (PEB), which is a PDA-sized device that can be inserted to a slot in the iVotronic. The PEB then communicates to the iVotronic using infrared signals. There are two types of iVotronic terminals, distinguished by their color of either red or blue. Red terminals are for administrative purposes, usually limited to one per precinct, which programs PEBs with necessary information such as election precinct ID, ballot design, and permissions. When a voter is authenticated and registered by a poll worker, the poll worker would accompany the voter to a blue iVotronic terminal and insert the PEB, which will allow the voter to vote once. Major security concerns revolve around the PEB coupled with buffer overflow vulnerabilities in the iVotronic software, allowing any attacker who can provide input to execute arbitrary code. The blue iVotronic terminal we analyzed can be seen in Figure 3.

Hardware Analysis

Our analysis begins with an inspection of the machine's exterior, followed by disassembly to inspect its interior in order to identify security risks and components of interest, for both the WinVote and iVotronic.

1. WinVote

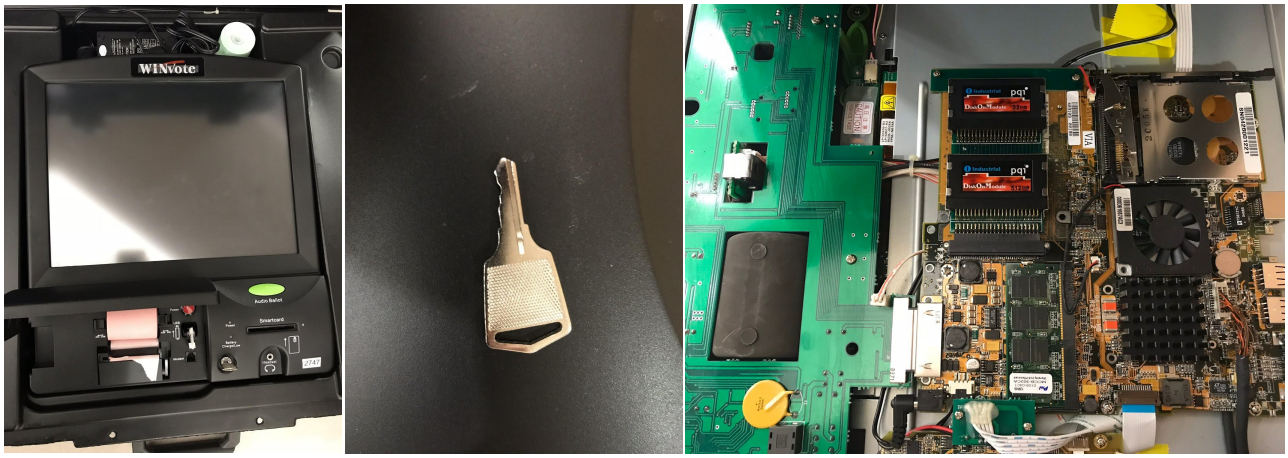

Figure 2. From left to right: The front face of the WinVote voting machine; the key from the panel; removed back panel and machine internals.

Specification. The WinVote was relatively easy to work with. The front of the machine consisted of a touchscreen, a port for a voting SmartCard, a headphone jack, a button for an audio ballot, indicator lights, a slot for a key, and a panel locked by the key. Under the panel, there was a USB stick held in place with a zip tie, a roll of receipt paper, a modem port, and the machine's power button. The rear of the machine contained two USB ports, a serial port, and an ethernet port. The back panel of the machine was held in place by ten Phillips screws and a ribbon cable, which connected the main board to the rear I/O. When removed and disconnected, the internals of the machine greatly resembled that of a laptop, with a Wi-Fi card, RAM in the SODIMM (small-outline dual in-line memory module) form factor, and a portable power supply. The motherboard also contained two disks in the IDE form factor secured with metal brackets, one of size 32 MB and the other of size 512 MB. The components can be seen in Figure 2.

Analysis. There were no security measures in place for the hardware. The machine can be simply disassembled and all components were found intact. The key locking the panel seems fairly insecure, and it wouldn't be surprising if all WinVote front panels can be unlocked by the same key. An attacker can simply replicate this key by purchasing one machine. The USB stick holding audit data is held in place with a plain white zip tie with no serial numbers, which an attacker can quickly remove and replace. There are also many easily accessible exposed ports, such as the rear USB ports and ethernet port. Disassembling the machine shows many components of interest, namely the disks, which we further analyze in following sections. It is worth noting that the disks are manufactured by PQI, a Chinese company, and are made in Taiwan, while the wireless LAN card is manufactured by Aaxxess, a Canadian company. All of this information is useful to attackers seeking to mount hardware or supply chain attacks.

2. iVotronic

Figure 3. From left to right: iVotronic voting machine, in case with privacy shroud; machine internals; CompactFlash card from the machine.

Specification. The exterior of the machine was rather featureless, containing only infrared sensors, four buttons on the front, a memory card slot, a serial port, and a power port for the rear I/O. There was a slot in the top of the machine for a Compact Flash memory card, which would hold audit data and any files that are too large for the main disk, such as audio files and ballot design. The Compact Flash can be easily removed. The iVotronic was more difficult to disassemble compared to the WinVote. The internals resemble a laptop, with the machine containing a ~6000 mAh battery, two visible flash chips, a large capacitor, and an old Intel i386 processor without any form of cooling. There are four non-volatile flash memory units. We knew from previous studies that one flash memory should contain operating system software, and the rest contains voting data in triple redundancy. Although analyzing these flash memory units would be ideal, they cannot be removed from the board. We resorted to analyzing the Compact Flash since at the end of the election day, the iVotronic copies data from flash memory to the card. The components mentioned can be seen in Figure 3.

Analysis. The rear panel was secured in place with nine Torx T10 security screws, which were slotted in very deep, narrow channels. Our screwdrivers were too wide to fit, so we were forced to drop the bit inside and rotate it with pliers until we could remove the screws. Although not much of an actual security measure, this will increase the difficulty for attackers under time pressure, such as during a voting day. The biggest security concerns is the easily removed Compact Flash, which would contain very sensitive data if removed during an election. A seal should be in place to guard against this, but seals used in elections are easily removed and replaced, and it is unlikely for election officials to inspect this small seal at the top of the iVotronic. Another major security concern is the PEB slot coupled with the iVotronic's buffer overflow vulnerabilities. An attacker with access to a used iVotronic would be able to develop malicious PEBs to limitless efficacy. If the attacker can successfully insert just one of these PEBs in a precinct, they can steal voting data and infect the terminal with malware, which will then spread quickly since poll workers will insert their own PEBs.

Software Live Analysis

Once we had a good understanding of how the machines were built, we wanted to see what they would do when they were booted. We hoped to get a look at the voting software, see how it would perform, cast a ballot, and see if we could access any voting records or logs.

1. WinVote

The WinVote did not boot, instead showing an error screen with the message "NTLDR is missing", which indicated that some crucial Windows boot files are either missing or corrupt. This could potentially be a result of an intentional security measure to wipe the drive prior to selling the machine. The screen also indicated that the key combination "ctrl-alt-del" could be pressed to restart the machine, so we plugged a USB keyboard into one of the rear ports. Restarting in this manner produced the same error screen, but holding the delete key after restarting allowed us to boot into the machine's BIOS settings. The BIOS settings allowed us to change a variety of hardware settings, including memory timings and boot orders. Although we tried to change these settings to get the machine to boot, we were unable to do so. An important security consideration is that the WinVote enables booting from USB. If an attacker can turn off the machine, enable this setting, and insert a specifically tailored disk to one of the WinVote's exposed USB ports, they would be able to compromise all data in the machine. Our attempts to boot up the WinVote can be seen in Figure 4.

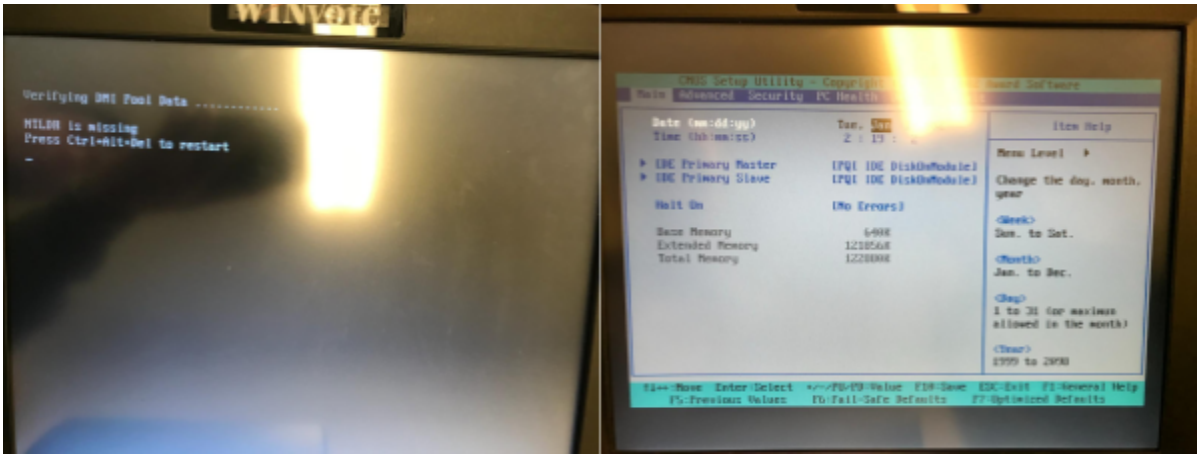

Figure 4. Left: WinVote error message. Right: BIOS main menu. Note the option to change IDE disk settings.

2. iVotronic

We were unable to boot the iVotronic to run its voting software, even though it could charge and turn on. We found that to boot the machine to its voting software requires a special poll worker PEB. Past work has indicated that the iVotronic PEB can be emulated using a PalmPilot PDA and some household magnets. However, we did not opt to do this because in addition to developing the PEB hardware, we would also need to program it to authenticate and emulate an admin PEB, which is outside the scope of our study.

Software Dead Analysis

In this section we proceed to perform dead analysis on the identified memory units of both the WinVote and iVotronic. Although we cannot successfully boot up either machine, the memory units should allow us to recover some data. We used Autopsy version 4.9.0, a free digital forensics software.

1. WinVote

sCandidateNumber	sFirstName	sMiddleName	sLastName	sNickName	sFullName
REINHOLD	GULKE		REINHOLD GULKE		121
GRAY	DAVIS		GRAY DAVIS *		111
IRIS	ADAM		IRIS ADAM	119	-1
PETER MIGUEL	CAMEJO		PETER MIGUEL CAMEJO		115
GARY DAVID	COPELAND		GARY DAVID COPELAND		113
BILL	SIMON		BILL SIMON	117	-1
PAUL JERRY	HANNOSH		PAUL JERRY HANNOSH		144
BRUCE	MCPHERSON		BRUCE MCPHERSON		139
KALEE	PRZYBYLAK		KALEE PRZYBYLAK		140
CRUZ M.	BUSTAMANTE		CRUZ M. BUSTAMANTE *		134
JIM	KING		JIM KING	142	-1

134	NA	NA	NA	(703) 913-8800	NA
135	NA	NA	NA	(703) 339-6572	NA
136	NA	NA	NA	(703) 780-5310	NA
137	NA	NA	NA	(703) 426-5280	NA
138	NA	NA	NA	(703) 506-7800	NA
139	NA	NA	NA	(703) 207-2390	NA
140	NA	NA	NA	(706) 876-5225	NA
141	NA	NA	NA	(703) 572-4202	NA
142	NA	NA	NA	(703) 714-5400	NA
143	NA	NA	NA	(703) 937-1600	NA
144	NA	NA	NA	(703) 560-5262	NA
145	NA	NA	NA	(703) 645-6300	NA
146	NA	NA	NA	(703) 645-6600	NA
147	NA	NA	NA	(703) 206-5300	NA
148	NA	NA	NA	(703) 208-8100	NA

1	N/A				
2	7604 Herald St.	Annandale	22003	Virginia	
3	4414 Holborn Ave.	Annandale	22003	Virginia	
4	5815 Ox Road	Fairfax Station		22039	
5	7825 Heritage Dr.	Annandale	22003	Virginia	
6	5400 Harrow Way	Springfield	22151	Virginia	
7	9524 Old Creek Drive	Fairfax	22032	Virginia	
8	7602 Heming Ct.	Springfield	22151	Virginia	
9	4910 Willet Dr.	Annandale	22003	Virginia	
10	5411 Nutting Dr.	Springfield	22151	Virginia	
11	4011 Iva Lane	Fairfax	22032	Virginia	
12	9525 Main St.	Fairfax	22031	Virginia	
13	9200 Burke Lake Rd.	Burke	22015	Virginia	
14	10110 Commonwealth Blvd.		Fairfax	22032	
15	5004 Sideburn Rd.	Fairfax	22032	Virginia	
16	10900 Santa Clara Dr.	Fairfax	22030	Virginia	
17	5035 Sideburn Road	Fairfax	22032	Virginia	
18	4511 Olley Lane	Fairfax	22032	Virginia	
19	5420 Sideburn Road	Fairfax	22032	Virginia	
20	5701 Roberts Pky.	Burke	22015	Virginia	

Figure 5. From top to bottom: Portion of the California candidates; portion of phone numbers found in the Virginia databases; portion of addresses found in the Virginia databases.

For the WinVote, as identified in the hardware analysis section, we analyzed the two disks in the machine internals as well as the USB stick zip-tied to the front panel. We imaged all of the disks we found using Autopsy. When the disk is first imaged, all of the data on it is read sector by sector to create a virtual disk image with a file extension .vhd, which Windows recognizes as a virtual hard drive. Windows can attempt to mount the drive or open it as a folder, which we tried. The WinVote could be mounted, although some folders would not open or were empty. This is to be expected since we found in the live analysis section that this machine likely had its drive wiped. When viewed in Autopsy every file could be seen as reconstructed; the software works by scanning each byte for recognizable file headers, and if it finds a header or a partial file header, it can recreate a file pointer for the deleted file. The software recognizes many different file formats, including images, audio, text documents, database files, and compressed archives to name a few. It was this reconstruction that allowed us to view the wiped drives for the WinVote.

The 32 MB disk contained a Windows XP Embedded installation with no service packs. However, we were more interested in the 512 MB disk, which contained all of the WinVote software along with the voter data. The data was spread across fifteen Microsoft Access databases (.mdb files) and two zip archives. Two mdb files corresponded to California elections, nine corresponded to Virginia elections, three contained junk data, and the last mdb file and both zip archives contained voting machine and ballot audit data. The California election took place in 2002, and was for multiple races. One database (f0100544.mdb) contained the races and candidates, some of which can be seen in Figure 5, while the second (f0118806.mdb) contained ballot data, including ballot type, ballot format, whether it was cast as absentee, and so on. There wasn't enough data across these two databases to determine where the machine was used, nor to match votes to individual voters.

We were able to discern that there were at least two Virginia elections, again for numerous races, that took place in 2012 and 2014. Every database contained phone numbers and addresses for registered voters, some of which can be seen in Figure 5. The addresses are full street addresses with house number, street, city, and zip code, and correspond to the cities of Annandale, Fairfax Station, Springfield, Burke, Vienna, Reston, Herndon, McLean, Great Falls, Falls Church, Alexandria, Lorton, Oakton, Clifton, Centreville, and Chantilly in Fairfax County, Virginia. All of the phone numbers have the area code (703) which corresponds to northern Virginia, except for one which had (706), which corresponds to Georgia. Nearly every database had candidate names. Something to note is that some databases had only Democratic candidate names, while others had all candidates; there were no databases that had Republican candidates, or candidates with other party affiliations. With all of the information present, were we given a record of who entered the polling station in what order, we would likely be able to reconstruct a complete record of who voted in which way.

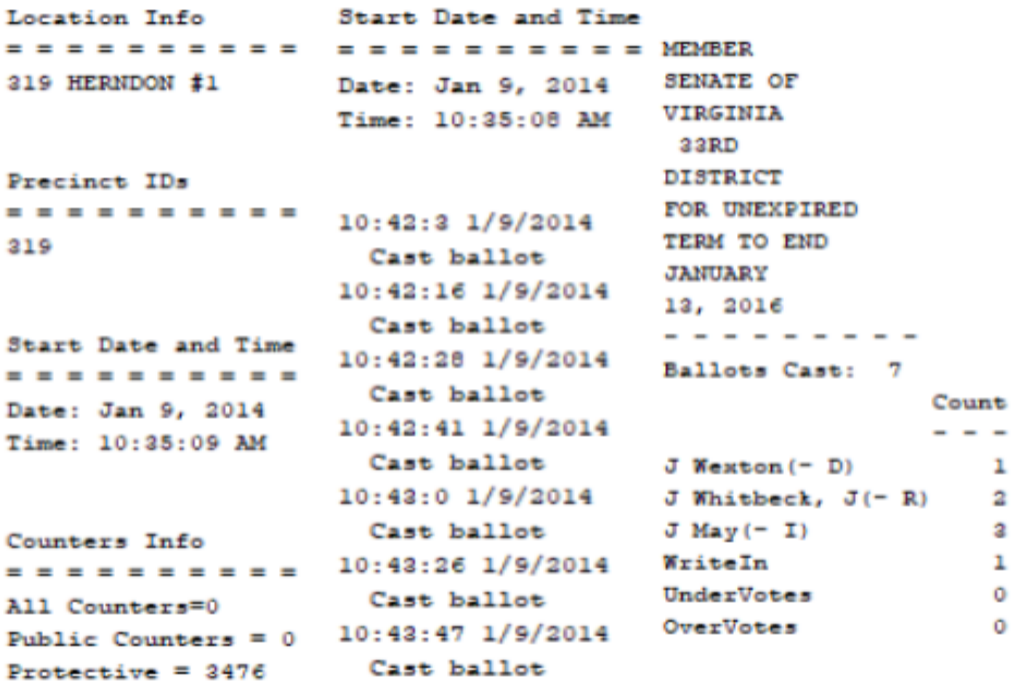

Figure 6. From left to right: Poll zero tape; presumed test votes by an election official; poll closing tape.

The WinVote machine we investigated had the serial number WV002747. The two zip files and the final database, when unpacked, revealed data from three different WinVote machines in addition to this one: WV001260, WV001644, and WV001802 all had ballot audit data contained on our machine. We believe this is due to how WinVote machines transfer data through wireless LAN between each other during elections. Since the logs are dated January 2014, we also believe that these four WinVote machines were in the same polling place during the January special election in Fairfax County. The files we found are a security concern because attackers would be able to identify the machines which are in the same precinct. Based on the U.S. election process, attackers would likely target specific swing states and precincts.

When unpacking database files we also found files containing the poll zero tape and the closing tape of what seems to be a test election by election officials during voting day, as shown in Figure 5. The zero tape is a security mechanism, and an attacker who can install malware would want this knowledge to produce a zero tape that is the least suspicious. We believe that the closing tape is a part of a testing process because only 7 ballots were cast and there were very short time intervals in between. The election official also made sure to cast at least one ballot for each candidate, and one write in candidate. This information is useful for attackers developing malware, presumably to switch votes between candidates. Using this information, the malware can be developed to detect specific characteristics that distinguish a real election from a test election, such as the short time intervals between ballots cast, number of ballots cast, and the candidates voted for.

Past research indicates that some WinVote machines contain audio ripping software as well as a Chinese mp3 titled “白雪-千古绝唱.mp3” (White snow - eternal singer). Autopsy was unable to reconstruct any music files on our machine, and a regular expression search revealed nothing related to audio software or any mp3 files.

2. iVotronic

As we imaged the iVotronic Compact Flash card and explored its contents, we found that the card likely did not belong to the original iVotronic. This is because it contained various files and data which should not be there, including several images, a song, and an executable, see Figures 7 and 8. Based on the files we found, we believe that the Compact Flash likely belongs to Professor Halderman’s research group, which provided us with the machine. This hypothesis is further supported by a variety of factors -- we could not find any voting data, which should be copied to the Compact Flash after an election day. The card memory size of 32GB is also much bigger than the expected few hundred megabytes.

Figure 7. Screenshot of the Autopsy image of the iVotronic’s memory card. Highlighted is “Hail to the Victors” in the .wav format.

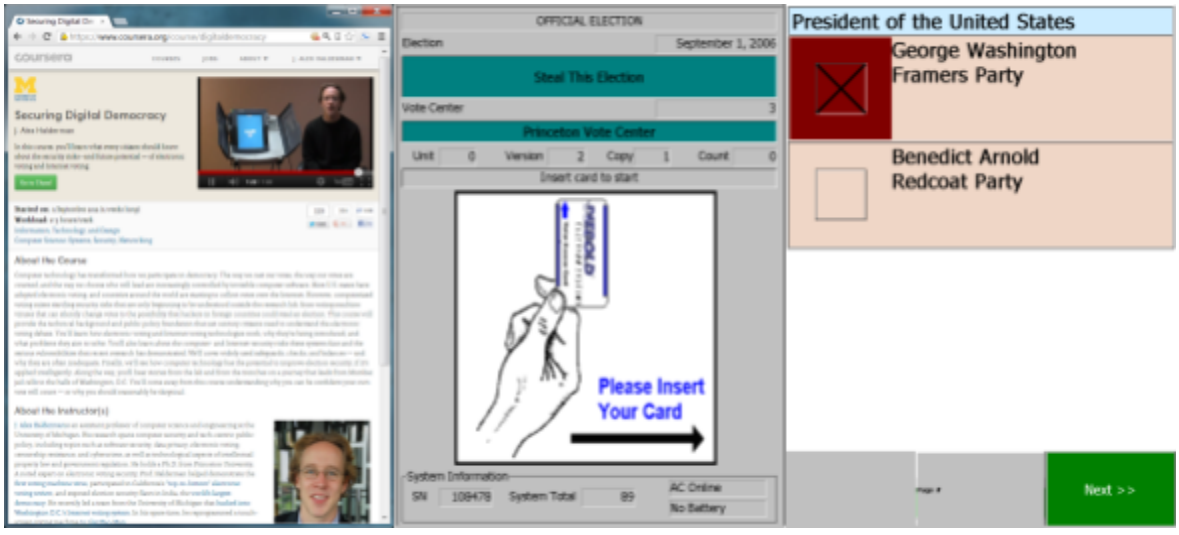

Figure 8. Images found on the memory card. From left to right: image5.bmp, image10.bmp, and image20.bmp respectively.

Conclusion

In this study, we have presented our grounds up exploration of the WinVote and iVotronic as obtained from online shopping platforms. Our forensic analysis utilize no special resources such as voting software source code, binaries, or anything else not publicly available, and we thus operate under similar conditions to potential attackers. Throughout our analysis we present our observations and analysis on how various pieces of information can aid attackers for future attempts to jeopardize the election process. We also present our findings on recovered data that represents a threat to election ballot secrecy and confidentiality. From our findings we recommend that used voting machines, even after having its drive wiped, should not be publicly available.

There are a few improvements and possible future work to extend this study. We hope to get WinVote and iVotronic machines that can successfully boot its voting software, which should not be difficult since drive wiping all voting machines is presumably a manual human-error prone process. We also hope to be able to further analyze the iVotronic by developing ways to access the flash memory units, obtaining PEBs, and obtaining the original Compact Flash card which were used with the machine. In addition, our study would be greatly helped by analyzing a wider range of models and a greater quantity of machines.

References

1. A. Aviv, P. Cerny, S. Clark, E. Cronin, G. Shah, M. Sherr, M. Blaze. “Security Evaluation of ES&S Voting Machines and Election Management System” https://www.usenix.org/legacy/event/evt08/tech/full_papers/aviv/aviv.pdf

2. A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. Medeiros, G. Tyson, M. Shamos, M. Burmester. “Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware” https://people.eecs.berkeley.edu/~daw/papers/sarasota07.pdf

3. Carsten Schuermann. “A Comparative Forensic Analysis of WinVote Voting Machines.” https://demtech.dk/publications/talks/blackhat-18.pdf

4. Released by Ohio Secretary of State, Jennifer Bruner. “EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing” https://www.eac.gov/assets/1/28/EVEREST.pdf

5. Verified Voting Foundation, Inc. https://www.verifiedvoting.org/

6. Virginia Information Technologies Agency. “Security Assessment of WinVote Voting Equipment for Department of Elections.” https://www.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf