DEFCON'S VOTING VILLAGE 2018

(Aug 10-12, 2018)
Summary notes from organizers

DAY 1

R00tz

- 39 kids from ages 6 - 17 attempted to hack replicas of the SOS websites of 6 swing states; 35 kids were able to complete an exploit. The quickest exploit was done by an 11 year-old in 10 minutes; kids were given an introductory walkthrough of how to perform an SQL injection. From there they ran with it and were able to complete the hacks.
- Kids tampered with vote tallies, party names, candidate names, etc; Total vote counts were changed to numbers like 12 billion and candidate names were changed to things like "Bob Da Builder" or "Richard Nixon's Head".

Voting Village

Diebold TSX

(Ed Note: Touchscreen system similar to the ones used STILL used across entire state of Georgia and other states)

- Active Diebold TSX voting machines were found to be running on expired SSL [security] certificates (2013) which makes these machines vulnerable to any vulnerabilities catalogued since then, and to hackers who could exploit them specifically on these machines. Diebold machine locks are also easily hackable.
- A hacker was able to reprogram a Diebold TSX to play gifs and music after uploading a Linux operating system. While this can not be easily carried out in the time it may take a voter to vote, it illustrates the malleability of these systems.
- On an Accuvote TSX, a hacker, once getting inside a machine, was able to gain full admin access through the J-Tag which allowed them to have full admin access. This took the hacker 30 seconds, as he was familiar with the machine.

Diebold Express Poll 5000 (electronic poll book system)

- Poll Book Machines (Express Poll 5000) were found to be vulnerable to having their easily accessible memory cards removed from the top of the machine and replaced with a market-purchased copy pre-loaded with alternative voting poll information. This means that voters that attempt to vote at a polling place may find that they are no longer in the precincts records, or other voters could be added who could then vote in that polling place. The hack can easily be performed by a voter within 5-seconds using a distraction or by a poll worker with access to all machines.
- Poll Book Machines (Express Poll 5000) also keep supervisor passwords on these cards and they are listed in plain text. These poll book machines also keep personal records for all voters including last four of social security numbers, address, drivers license numbers and are completely unencoded.
- Expanding on the password details above: The hackers were able to read and write the database inside, using SQL lite (a simple database program available everywhere). They discovered that the root password and administrative password are stored in the device, in clear text. The root password is: **"password"** (Something we're all taught NOT to do). While exploiting this vulnerability would require physical access to the pollbooks to make use of the info, it's entirely possible to do. The real security failure is that the passwords are stored in clear text in the machine.

ES&S

- ES&S Vote Counter machines, the kind used by counties to count ballots from municipalities, were found to have active ethernet ports, exposing them to several vulnerabilities.
- ES&S m650 [*Ed Note: Widely used in more than half the country for absentee ballot tabulation*] - The hacker had never seen the machine before today. He discovered that if you remove the back panel, that there is a port there that he could completely control the machine from. He was able to get serial console access to the machine. The machine is running a version of QNX operating system, that is a multi user operating system but that was configured for only one user (the root user) and that there was NO password. The machine has a very accessible zip drive on the front of the machine. In order to update the software, you insert a zip disc that has the new copies of the software. You can create corrupted version of software, add to a zip disk, and insert it, which will override the software on the machine. There is NO check that the software is genuine. The software *should* have digital signature, which it would check, before doing any update. The machine does not have this.
    - The danger here is that you can create a corrupted version of the software which will not only corrupt the machine, but when you insert a good zip disk, the machine can infect that zip disk, which if inserted into others will cause a viral spread of the infected software.

    - This vulnerability was discovered years ago, but it was not published. *[Ed Note: Just one of the issues with these machines redacted from publicly released security analyses over the years.]*

Cyber Range (Voter Registration Database)

- The Cyber Range project was a simulation of a state's voter registration database that hackers attempted to break into and modify. One hacker was literally one step away from totally compromising the system in the short time the hacker was working to compromise the system, which unlike hacking voting machines, can be done over a longer period of time.
- Last year, the cyber range was penetrated in 10 minutes. This year, it deployed a security code used by foreign military [Israeli military encryption, as I understand it] to make it harder to penetrate. And it was still almost penetrated.

DAY 2

R00tz Asylum x Voting Village

- Awards
    - There were three age group categories for the awards: Under 11; 12-14; and over 15
    - Fastest: Emmet, 11, 10 mins; Joel, 13, under 15 mins; Seth, 16
    - Most Innovative: Audrey, 11; Nik, 13; Szczepan, 15
    - Most Social Engineering: Jonathan 11; Reina 14; Celie 16
    - Youngest Exploiter: Sophie 10; Sarah 12; Nora 15
- One kid changed the candidates to Kim Jong Un, and gave him a billion votes.
- Other hacks (changed "Donald Trump" to "Tonald Drump")
- Over the course the two days there were a total of 50 kids that participated in the hacking.

Voting Village

- The Village hosted an election, facilitated by Alex Halderman, and it was (unsurprisingly) hacked
    - Voters at the conference were given two choices of candidates to vote for, one being George Washington and the other being Benedict Arnold. 133 ballots were cast, and the winner was The Dark Tangent, a third candidate who received 61 voters to 26 each for Arnold and Washington. The hack was done on an AccuVote TSX, which is used in 18 states, some with the same software version. The hack was accomplished by reprogramming the memory cards on the machine in advance to predetermine the result, but still based on the number of ballots cast.
- On an Accuvote TSX, a hacker, once getting inside a machine, was able to gain access through the J-Tag which allowed them to have full admin access. This took the hacker 30 seconds, as he was familiar with the machine.
- WinVote, Machine #2664: Controlled a music player on a laptop from the voting machine
    - VoteActive Machines could be accessed with an exploit in seconds wirelessly. Vote counts were changed.
    - Within the master image file of the software, which runs on Windows XP, files were discovered installed by the manufacturer. These files included a Chinese pop-song, by an artist known as Cascada-Dangerous called 'Loveyou'
    - Also discovered on the WinVote was a cd ripper program.
    - There were also files related to a music playing program, Coolplayer, which appear to be Chinese in origin.
    - The hacker found that there are non-windows programs on the machine, in addition to Coolplayer, one being some program called Kicker, whose purpose is unknown, but it demonstrates that external programs can easily be uploaded to the machine.
    - These machines have been used for several years, but they've never been reformatted, not even when they were new. We knew that because the song that was discovered was a deleted file. If the machine had been reformatted the song would not have been there.
    - The Village also learned that the FTP log files on the machine show that there were unencrypted transfers of the full database of the machine to a server, which is FTP.enfocom.com. The company (Enfocom) is (now) located in Calgary, Canada. The IP address was [REDACTED for now pending further investigation]. The point is, we don't know why the database was sent in the first place.
    - All machines of this type are networked together when in the same polling place.

ES&S M650

- The ESS machine, M650, was hacked again in a similar manner from yesterday. They discovered a buffer overflow, but it was not exploitable. This buffer overflow was in the DHCP server.

- This is now a total of two vulnerabilities identified in this machine

An email ballot was hacked.

- The selection of the candidate was changed so that when it was received it was different from what was sent.
- The ballot left the sender, and it was not hacked until it was received by the receiver. The email server is modular and is built to allow various filters. The hackers added a filter that hacked the message, changing the candidate selection.
- This was all done in 2 hours from when the first command was written to the final execution.
- This is a big deal for the real world because we already allow for email balloting, in special cases for Americans living overseas. This is allowed in 30 states plus DC.

Polling Express 5000 (Windows CE 2.0.27)

- A user plugged an easily accessible flash card into the reader, mounted it on a standard laptop, modified the contents, and re-uploaded it to the computer. Also, the cards are standard SanDisk models, which means they can be purchased and programmed in advance.
- Hackers were able to add a voter, delete a voter, change a voter's status to having already voted before Election Day, replace the map of the voter's voting location with a jpg/meme.

DAY 3

Voting Village

- The Diebold TSX, which is from the early 2000s, has had legacy data exfiltrated, meaning it was not wiped clean. The analysis on this is continuing.
- Hackers have continued working on the ES&S m650. It was discovered that any file named "update" on an inserted zip disk will immediately be executed at the highest privileged level. Normally, that would be an update installer but it, can in fact, be literally any program. While we already knew that we could use the zip drive to install new code, this is a shorter method of running arbitrary code.
- On the WinVote, it is incredibly easy to jimmy the lock, meaning that someone would have full access to the machine relatively easily. Also found on all 16 of the WinVote disk images were 1784 deleted files, using basic terminal commands.