ES&S DS200 Wireless Vulnerabilities

Jill and I have been on the trail of a series of clues showing that wireless subversion of vote totals and election processes is possible and is occuring in the field. People known to be involved in past election fraud efforts have been tracked hiring staff to build a wireless communication "interruptor". Subversion of cellular communications by both law enforcement and criminals is a well understood field and the entire United States government from FBI Director Comey on down have denied that ties to the general Internet from voting machines exist. As we'll show, Comey lied to the general public *and congress* on this key point. We're going to show the extent of the problem and the security implications. We are calling for an immediate ban on the use of wireless communications in election machines and a security review of the ES&S DS200 and other newer-generation voting machines that have not been subjected to any "red team attack" ("penetration testing") security reviews.

The DS200 is an optical scan ballot processing device that is in broad use across the country; it's fairly small and slow and is therefore meant for precinct duty or in smaller counties it can process the mail-in votes. It is a "graphic scanner" as opposed to the old mark-sense technology and is capable of storing the ballot image files that it scans. However, ES&S included an easily accessible software switch that allows election administrators to destroy the graphic images immediately after they're scanned and the voter intent is processed – a questionable feature at best.

Of equal concern however is wireless modems shipped with the machines or in some cases added after the fact, and the implications for that data communication from the field when viewed as proof there is an online gateway into each county's "crown jewels" - *the one machine per county that tallies the vote and reports the final official numbers*. That device shouldn't be externally accessible at all, but to facilitate in-bound data streams from the DS200 on election night, a dangerous connection must be created.

This project was made possible by funding gratefully received from AUDIT AZ, Protect our Vote, RecountNow.org TrustVote.org all working being the "WE". AS you know that how hard that is to do. After realizing that 24 out of 72 counties were going to only machine count we broke into two teams focusing mainly the counties that were machine counting ballots. Team 1 was John Brakey and Chris Sautter" Team 2 was Jim March Simpson and Jill Simpson This investigation started in Wisconsin due to the recount the Stein campaign ordered and happened with the collaboration of John Brakey of AUDIT-AZ and the Green Party of Wisconsin and the national-level Green Party.

After several days on the road John Brakey questioning election official in Milwaukee and asking how the results from the precincts/wards were transferred from the ES&S DS200 to the Election Management System "EMS". Brakey asked "How do you transfer the results, by soft shoe network, or telephone landline modem or SIM card. The official said "SIM card". Immediately after that John Brakey contacted team 2 and Jim March Simpson who is one of the best geeks in the field and asked him to investigate the cellular network system.

A point about the Wisonsin recount: doing a machine recount of votes is like asking for a 2nd receipt from a deposit at an ATM machine. It's EXACTLY the same except you can trust the ATM because it tied to an account, it is not anonymous and is audited daily. Elections are a very different matter!

Chapter 1: Understanding the Architecture (and central vote total vulnerabilities)

Per our discussions with county election officials in Wisconsin and other digging current and past we have established the following facts:

> * On election night the precinct (actually “ward” in WI) voting machines send data to the central vote counting location (and machines) via the wireless connection – and this connection is started by the pollworker in the field. *This is an important detail we’ll come back to in a bit.*
>
> * The connection goes through the Verizon wireless network and into the central vote count location through a “VPN” - Virtual Private Network. A VPN is a method corporations often use to create secure inbound connections, for example allowing a work-at-home employee to securely get to the company’s internal computer systems that are not otherwise Internet-facing.
>
> * The actual setup of this VPN connection was facilitated by ES&S – all of the county election staff and techs we talked to were fuzzy on the exact details but threw around a lot of buzzwords like “router” and “firewall”. Worse, all assured me that the WI state election board people who allow specific voting machines to be purchased and used in WI “would have checked all that” - all used words more or less to that effect. (We have multiple examples on audio.) The most technically detailed information came by conference call with a county IT staffer in Sauk County who was at least certain that VPN technology was in use.
>
> * A “firewall” is, best case, a device that sits between one or more computers you want to remain secure and the general Internet. It allows people inside the secure area to make contact with the Internet while blocking inbound connections from evil hackers from the general Internet...basically a one-way filter. Remember how I said that the DS200s were *initiating* the connection? That means inbound connections are possible. Yes, there’s security of some sort, and yes a VPN connection *can* be built quite solidly. But the security in this case is not tested and is of an unknown type that the county election official customers don’t seem to understand.
>
> * When we were finally able to ask one of the state-level voting system testing and approval people about this, that person told us that no, there was no “penetration testing” (ie: “test hacking” to check for vulnerabilities) and that they relied on the **Federal** voting system certification system and testing process to do that sort of analysis. (Yes, we have this on audio as well.)
>
> * From our own examination of the federal test lab and certification systems, we can state authoritatively that they aren’t checking either!
>
> * The only official penetration testing that we are aware of were the “red team attacks” authorized by the state of California in 2006 – and the DS200 didn’t ship until 2011: http://electiondefensealliance.org/ca_voting_systems_overview_red_team_reports

Upshot: *in order to allow cellular data communication, opening an entry point into the central vote counting systems has to happen.*

Can that entry point be exploited?

It is common for serious system administrators to understand “black hat hacking” techniques so as to be able to prevent them, although this mindset is almost completely missing in election security thinking! The literature on exploiting VPN connections flourishes. From the standpoint of a “lone wolf” hacker, it’s possible to determine which VPN security products are in play and attack known vulnerabilities:

http://www.h-online.com/security/features/Breaking-into-a-VPN-747175.html

What a determined attacker with government-level resources can do is much more frightening: http://arstechnica.com/security/2015/10/how-the-nsa-can-break-trillions-of-encrypted-web-and-vpn-connections/

That's what our own government can do. I don't think we're the only ones with this class of capability…the Russians and Chinese are well known players in this field. The British, Germans, Israelis and many others aren't that far behind.

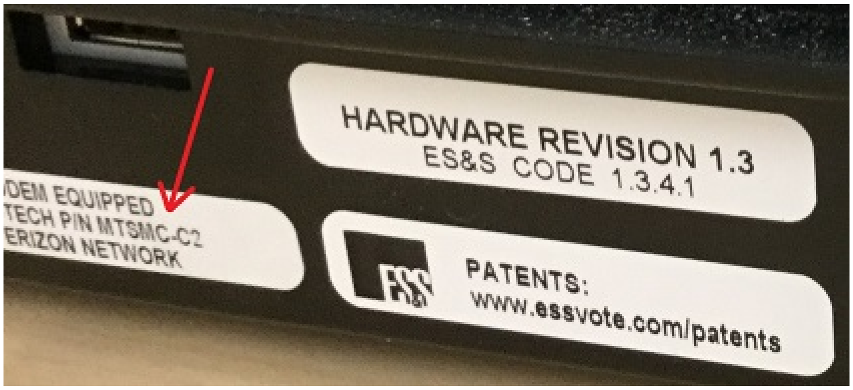
Pay attention to the sheer number (percentages) of VPN systems vulnerable should the NSA throw significant resources into cracking a small number of cryptographic key supports (last link above).

Would such an exploit (remote alteration of vote totals in the central count) pay off in terms of an actual altered election result?

In Wisconsin there are some good points to the election process that would make such an exploit difficult. The state requires each county to save the digital images of each ballot at the DS200 and optional DS850 (high speed version) scanner. These ballots are available as a public record. Knowing this, informed party officials for example can double-check elections and just the known ability to do so will likely dissuade at least some would-be election hackers.

However, in the state of Iowa there is no legal access to these ballot images. In Ohio numerous jurisdictions are destroying them after use. In Colorado insane financial barriers to access are widespread...and so on. If the original paper ballots cannot be referenced after the fact without an expensive challenge and the graphic images aren't available (or are destroyed), tampering with the central electronic records can subvert the election.

Chapter 2: Vulnerabilities at the precinct machine level (direct cellular hacking)



In St. Croix County WI there was a visible tamper evident seal in place on one of the screws that lead into the "guts" of the device. Various concerned people took pictures of the machines in question and one picture (as seen on the right) poses obvious questions. The red arrow points to the make and model of an internal cellular modem. Here's the data sheet: http://www.multitech.com/documents/publications/data-sheets/86002156.pdf

If we look on page two we see "TCP/IP Functions" - "DNS Resolve" means it can hit websites, FTP means "File Transfer Protocol" (on the Internet), POP3 means Email while PPP is about doing a direct connection between two machines, often over the general Internet and is likely how ES&S has these machines at least try and maintain a connection back to their own county's home base central tabulator station. This is a full-tilt Internet-capable cellular modem.

We know that the device used in Wisconsin uses the Verizon network and there's a report from Florida showing the same thing is approved – note that it was tested purely for functionality, not for security:

http://dos.myflorida.com/media/695182/ess-evs-release-4500-version-4-revision-1-test-report.pdf

There's references there to versions for other cellular networks (Sprint, AT&T, etc.). So far we're seeing Verizon in Wisconsin and Florida but we've just started down this rabbit hole.

Implications:

A few years ago Jill was tipped that there was an individual running advertizing at the monster.com job board for people who could "interrupt" wireless data communications once fraud was detected. Jill knew who this was and started tracking it in terms of whether or not it could be adapted to election fraud, working with attorney Cliff Arnbeck in Ohio. Now that we know cellular data communications in election results is in play, we can see how this class of technology could be adapted to election fraud. This could also affect pollbooks and the rest of the election infrastructure. Jill also went to the ES&S offices this summer to look at their patent wall and see what was relevant to wireless tech.

Let's put a few more pieces together. There's an infamous device in use by law enforcement called a "Stingray" by the Harris corporation: https://www.extremetech.com/mobile/202935-new-york-police-caught-lying-over-stingray-use-spying-without-court-oversight

The Stingray works by faking being a cell phone tower and getting nearby cellphones to jump to it – at which point the traffic back and forth to those phones can be intercepted. The Stingray is a big expensive critter in large part because it's range is fairly massive – it's meant to be plugged into serious antennas. So do smaller versions exist? Sadly, yes:
http://www.digitaltrends.com/mobile/femtocell-verizon-hack/

The short form is that Verizon makes a cellular range extender for $250. You plug it into an Internet connection and it becomes a tiny little cell tower by design. A hacked version can tamper with the data streams in and out of nearby cellphones – basically a budget Stingray with a range of 15 to 40 feet. Put a slightly better antenna on it, put it in a backpack with a power supply and cellular-to-Ethernet gateway device and you could do a lot to a DS200-based election. This is what can be done on an extreme budget – there's no telling what hackers with the resources of, say, the Russian government or for that matter the NSA can do.

Important: if you read the literature we cite on VPN hacking, one known attack method is to intercept the "hash" of the password that the voting machine in the field uses to initiate the connection back to home base and then "crack the hash" - in other words use brute-force methods to compare the hash (encrypted password) with long lists of known passwords such as dictionary words, dictionary words with numbers added, upper and lower-case variants, etc. Therefore, in theory an attacker doesn't need to raid the cellular connections at ALL the precincts with multiple "budget Stingrays". You only need one!

"Cracking the hash" is still a mathematically difficult challenge but it's been made easier of late by the fact that serious game-grade video cards can be used to do massive levels of calulation...and you can also use a bunch at once if you're really serious. See also:
http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

The term "Interrupter" does show up in cellular blocking technology which was part of what was being talked about: http://soaho2003.en.ec21.com/Cell_Phone_Signal_Interrupter--1942950.html

Jill has personally observed, in various Republican political offices, various ballots and **voting machines** including the latter being disassembled and evaluated for security issues. Those of us in the election protection community cannot get access to these machines to check for vulnerabilities and show defenses *but political operatives have full access* to understanding the intricacies of these systems.

(Note: we sometimes get access to older models that got put in storage and a government agency forgot to pay the storage fees at which point they turn up on Ebay(!). That's happened twice now.)

Other DS200 Security Issues

The DS200 has a standard socket inside for one of these cellular modem plug-in boards. It also has a USB port on the rear and USB is also likely accessible from the pinouts to the data socket for the cellmodem. There's three USB ports for memory sticks behind a locked door – that's how the ballot images are retained. These all provide a hardware attack surface to plug in illicit data and programs including the ability to switch the cellular modem to "full internet mode".

The DS200 saves graphic images to flash drives. Since that drive is removable it could have programming added via that card, if the security isn't set up correctly. Access to the insides of these devices is very easy; they use standard Torx security screw bits available any any decent hardware shop.

It's very important to remember that some counties are deliberately destroying the graphic scans of the ballots. In such jurisdictions a "man in the middle" attack against the cellular data connection in and out of these machines would be extremely dangerous as it could not be detected without detailed review of the paper ballots. *In Florida where this issue is in play, review of paper ballots once they've been scanned is flat-out illegal.*

We can find no evidence that anybody in government or the voting system test lab and certification systems have reviewed the security implications of the DS200 wireless capabilities. They tested to make sure the products worked together as ES&S intended but they didn't go to the next level and ask "what else can this stuff do?"

Did Comey Lie?

FBI Director Comey told the American people and specifically **Congress** that the US voting machines are not connected to the Internet. As we've seen, at least in the case of the extremely popular DS200 voting machine, that wasn't true. They are **physically** connected to the Internet, without question. ES&S would argue that there is a software block in place but as far as we can tell **nobody** has tested the efficiency of that block or checked to see if it can be subverted. Anything connected to the Internet is hackable if you find the right hacker and pay Verizon $250. *This is an intolerable situation.*

The Muske Affidavits

When we went to the St. Croix County Clerk on 12/6/16 they were unable to provide period-era maintenance documents for the machines that had broken tamper-evident seals into the guts of the machines. What they did instead was get an affidavit from the alleged sole tech from ES&S who came out to service the machines. There's two versions because on the first he apparently forgot a detail on paragraph 11 page 2.

The first thing that stands out is that this could be fabricated from top to bottom, or not – he might have based it on his own service records. He clearly got one detail wrong and had to fix it.

The second issue however is that he is clearly in there doing "modem things" just before each election cycle, which is suspicious in and of itself. We also see that at least this tech (and ES&S in general?)

was sloppy with security seals blocking access to the guts of the devices where significant other mischief can occur such as adding memory devices containing malicious programming.

Conclusion:

If the FBI reviewed these machines they could not have possibly stated that they were “not online”. This begs the question: did the FBI really do any review, or was it all just a lie so his candidate could win?

Jill and I feel that we’ve made a start at the security review Comey’s people should have done (and before that, the infamously dysfunctional voting system test lab and certification process).

We also want to point out that only during an exhaustive recount process like this can details of voting system security vulnerabilities be fleshed out. We are extremely thankful to the Jill Stein campaign for creating the conditions necessary to take a closer look at how elections actually happen.

Worst of all, we can see that opening the central vote count systems to outside contact via VPNs allows an entity with government-level resources to completely “own” the electoral process in states that don’t provide for adequate publicly-accessible checks and balances.

That in turn is an intolerable situation.

Appendix A: the Affidavit of Thomas Muske

four pages

COPY

STATE OF WISCONSIN

AFFIDAVIT OF THOMAS R. MUSKE

STATE OF NEBRASKA)
) ss.
DOUGLAS COUNTY)

Thomas R. Muske of St. Joseph, Minnesota, being first duly sworn on oath, states as follows:

1. I am a Senior Field Service Technician for Election Systems & Software, LLC located at 11208 John Galt Boulevard, Omaha, Nebraska 68137.

2. I have been employed by Election Systems & Software, LLC for 15 years.

3. My primary duties as a Senior Field Service Technician for Election Systems & Software, LLC are to repair and service Election Systems & Software, LLC's election system products.

4. Since 2015, I have been responsible for routine servicing of the election system scanning machines for various municipalities in St. Croix County, Wisconsin.

5. On multiple occasions, I serviced election system scanning machines in St. Croix County, Wisconsin, referred to as DS200 scanners.

6. On November 1, 2016, I serviced DS200 scanner Serial No. DS0314340857 for the Town of Springfield, St. Croix County, Wisconsin for a modem issue.

7. On November 16, 2016, I again serviced the DS200 scanner Serial No. DS0314340857 for the Town of Springfield, St. Croix County, Wisconsin on November 16, 2016 due to a lock that was out of alignment. I did not have replacement warranty labels with me at the time so the warranty label was not replaced.

8. On December 28, 2015, I serviced DS200 scanner Serial No. DS0315410032 for the Town of Troy, St. Croix County, Wisconsin for a modem issue that occurred during installation. I did not have replacement warranty labels with me at the time so the warranty labels were not replaced.

9. On December 28, 2015, I serviced DS200 scanner Serial No. DS0315410072 for the City of Hudson, St. Croix County, Wisconsin for a modem issue that occurred during installation. I did not have replacement warranty labels with me at the time so the warranty labels were not replaced.

10. On December 28, 2015, I serviced DS200 scanner Serial No. DS0315410021 for the City of Hudson, St. Croix County, Wisconsin for a modem issue that occurred during installation. I did not have replacement warranty labels with me at the time so the warranty labels were not replaced.

11. On December 28, 2015, I serviced DS200 scanner Serial No. DS0314350216 for the Town of Warren, St. Croix County, Wisconsin for a modem issue that occurred during installation. I did not have replacement warranty labels with me at the time so the warranty labels were not replaced.

12. In order to service a DS200 scanning machine and gain access to the inner workings of the machine, I use a security screwdriver that has been designed to open the scanner machine. This tool is needed as the election system scanning machines have special screws.

13. It is typical and customary to break the warranty labels on the DS200 scanning machines when servicing the machines.

14. The warranty label placed on the DS200 scanning machine is not the "security seal" on the machine as addressed in Wisconsin Statute § 7.25(6)(b)1.b. The warranty labels are used for Election Systems & Software LLC's internal purposes only.

15. The warranty is not voided when the warranty label is broken for the purposes of servicing the DS200 scanning machine.

12/5/16
Date

Tom Muske
Thomas R. Muske

Subscribed and sworn to before me this 5th day
of December, 2016.

Timothy J. Hallett
Notary Public, State of Nebraska

State of Nebraska - General Notary
TIMOTHY J. HALLETT
My Commission Expires
January 15, 2020

My commission expires: January 15, 2020

STATE OF WISCONSIN

AMENDED AFFIDAVIT OF THOMAS R. MUSKE

STATE OF NEBRASKA)
) ss.
DOUGLAS COUNTY)

Thomas R. Muske of St. Joseph, Minnesota, being first duly sworn on oath, states as follows:

1. I am a Senior Field Service Technician for Election Systems & Software, LLC located at 11208 John Galt Boulevard, Omaha, Nebraska 68137.

2. I have been employed by Election Systems & Software, LLC for 15 years.

3. My primary duties as a Senior Field Service Technician for Election Systems & Software, LLC are to repair and service Election Systems & Software, LLC's election system products.

4. Since 2015, I have been responsible for routine servicing of the election system scanning machines for various municipalities in St. Croix County, Wisconsin.

5. On multiple occasions, I serviced election system scanning machines in St. Croix County, Wisconsin, referred to as DS200 scanners.

6. On November 1, 2016, I serviced DS200 scanner Serial No. DS0314340857 for the Town of Springfield, St. Croix County, Wisconsin for a modem issue.

7. On November 16, 2016, I again serviced the DS200 scanner Serial No. DS0314340857 for the Town of Springfield, St. Croix County, Wisconsin on November 16, 2016 due to a lock that was out of alignment. I did not have replacement warranty labels with me at the time so the warranty label was not replaced.

8. On December 28, 2015, I serviced DS200 scanner Serial No. DS0315410032 for the Town of Troy, St. Croix County, Wisconsin for a modem issue that occurred during installation. I did not have replacement warranty labels with me at the time so the warranty labels were not replaced.

9. On December 28, 2015, I serviced DS200 scanner Serial No. DS0315410072 for the City of Hudson, St. Croix County, Wisconsin for a modem issue that occurred during installation. I did not have replacement warranty labels with me at the time so the warranty labels were not replaced.

10. On December 28, 2015, I serviced DS200 scanner Serial No. DS0315410021 for the City of Hudson, St. Croix County, Wisconsin for a modem issue that occurred during installation. I did not have replacement warranty labels with me at the time so the warranty labels were not replaced.

11. On December 28, 2015, I serviced DS200 scanner Serial No. DS0314350216 for the Town of Warren, St. Croix County, Wisconsin for a modem issue that occurred during installation. The label was broken during servicing the scanner. However, after servicing the scanner, I placed a yellow warranty label over the broken white warranty label.

12. In order to service a DS200 scanning machine and gain access to the inner workings of the machine, I use a security screwdriver that has been designed to open the scanner machine. This tool is needed as the election system scanning machines have special screws.

13. It is typical and customary to break the warranty labels on the DS200 scanning machines when servicing the machines.

14. The warranty label placed on the DS200 scanning machine is not the "security seal" on the machine as addressed in Wisconsin Statute § 7.25(6)(b)1.b. The warranty labels are used for Election Systems & Software LLC's internal purposes only.

15. The warranty is not voided when the warranty label is broken for the purposes of servicing the DS200 scanning machine.

12/5/16
Date

Thomas R. Muske

Subscribed and sworn to before me this 5th day
of December, 2016.

Timothy J Hallett
Notary Public, State of Nebraska

State of Nebraska - General Notary
TIMOTHY J. HALLETT
My Commission Expires
January 15, 2020

My commission expires: January 15, 2020