Adventures in Electronic Voting Research

Dan S. Wallach
Professor, Department of Computer Science
Rice Scholar, Baker Institute for Public Policy
Rice University
Many problems in voting!

Traditional concerns: vote casting, tallying, gerrymandering

Newer concerns: nation-state adversaries, misinformation

Today: Where we are, what’s next
Our story starts here.

The election is here.
Russian hackers targeted Arizona election system

The FBI says it has found breaches in voter registration systems in Illinois and Arizona, and it's urging states to increase their computer security ahead of the November presidential election. (Reuters)

By Ellen Nakashima August 29

Hackers targeted voter registration systems in Illinois and Arizona, and the FBI alerted Arizona officials in June that Russians were behind the assault on the election system in that state.

The bureau described the threat as "credible" and significant, "an eight on a scale of one to 10," Matt Roberts, a spokesman for Arizona Secretary of State Michele Reagan (R), said Monday. As a result, Reagan shut down the state's voter registration system for nearly a week.
WASHINGTON — The Obama administration on Friday formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee and a range of other institutions and prominent individuals, immediately raising the issue of whether President Obama would seek sanctions or other retaliation.
“33 states and 11 counties or local election officials” have requested help. (October 2016)

39 states compromised (June 2017)
Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known

by Michael Riley and Jordan Robertson
June 13, 2017, 4:00 AM CDT
The scope and sophistication so concerned Obama administration officials that they took an unprecedented step -- complaining directly to Moscow over a modern-day “red phone.” In October, two of the people said, the White House contacted the Kremlin on the back channel to offer detailed documents of what it said was Russia’s role in election meddling and to warn that the attacks risked setting off a broader conflict.
What did the Russians do?
Phishing 101

Spammed emails, trying to steal things from users

*Passwords / credentials*: useful for later hacking attacks (e.g., ransomware)

*Bank account data*: steal their money

Response rate is tiny, but the activity is still profitable

---

Dear Sir:

I have been requested by the Nigerian National Petroleum Company to contact you for assistance in resolving a matter. The Nigerian National Petroleum Company has recently concluded a large number of contracts for oil exploration in the sub-Sahara region. The contracts have immediately produced moneys equaling US$40,000,000. The Nigerian National Petroleum Company is desirous of oil exploration in other parts of the world, however, because of certain regulations of the Nigerian Government, it is unable to move these funds to another region.

You assistance is requested as a non-Nigerian citizen to assist the Nigerian National Petroleum Company, and also the Central Bank of Nigeria, in moving these funds out of Nigeria. If the funds can be transferred to your name, in your United States account, then you can forward the funds as directed by the Nigerian National Petroleum Company. In exchange for your accommodating services, the Nigerian National Petroleum Company would agree to allow you to retain 10%, or US$4 million of this amount.

...
“Spear phishing”

Phishing a specific person
Here, John Podesta (HRC’s campaign manager in 2016)

Spear phishing attempts are harder to automatically detect
Regular spam is high volume
Spear phishing emails are customized
WikiLeaks

Julian Assange: “hacktivist”
Early 2000’s, working on privacy technologies

http://caml.inria.fr/pub/ml-archives/caml-list/2000/08/6b8b195b3a25876e0789fe3db770db9f.en.html

WikiLeaks founded in 2006
“Collecting” and disseminating newsworthy information
One technique: Ran a Tor “exit node”, sifted through the data

Chelsea Manning leaks in 2007
“Collateral Murder” drone videos
https://www.commondreams.org/views/2015/04/04/five-years-wikileaks-collateral-murder-video-matters-more-ever
Russia + WikiLeaks

Assange denies it, but U.S. intelligence says:
Russian intel agencies collected on Hillary Clinton, DNC, etc.
  • Exact methods we don’t know
  • Definitely phishing, possibly other hacking techniques

Used WikiLeaks as a cut-out / front organization
  • Assange may well believe his sources weren’t Russian

Also: “DCLeaks” and “Guccifer 2.0”

July 2018: U.S. Special Counsel Mueller indicted 12 Russian GRU agents
Propaganda

Propaganda: Always a part of military strategy
“Win the hearts and minds”

Modern Russian military theory: “hybrid warfare”
Includes cyber attacks, propaganda, etc.

U.S. M105 Leaflet Bomb, 1950’s
Agitprop = Agitation + Propaganda

French anti-Jewish book, 1938

Russian anti-capitalist poster, post-Communist Revolution

German anti-American poster, WWII
Russian agitprop in the 2016 election

Russian agitprop in the 2016 election

Facebook ad, purchased by Russians

Russian agitprop in the 2016 election

Russian agitprop in the 2016 election

Russian agitprop in the 2016 election

Black people should wake up as soon as possible. Black families are divided and destroyed by mass incarceration and death of black men.

Targeting the American left as well.

“Texas Antifa”

Russian fake antifascist Facebook group
Threatened to remove Sam Houston statue in Hermann Park
Right-wing counter group (“This is Texas”) organized a rally in “defense”

https://www.thedailybeast.com/texas-conservatives-fall-for-anti-antifa-hoax
https://thinkprogress.org/hermann-park-protest-houston-28895d563f38/
“Texas Antifa”

Russian fake antifascist Facebook group
Threatened to remove Sam Houston statue in Hermann Park
Right-wing counter group (“This is Texas”) organized a rally in “defense”

https://www.thedailybeast.com/texas-conservatives-fall-for-anti-antifa-hoax
https://thinkprogress.org/hermann-park-protest-houston-28895d563f38/
“Texas Antifa”

Russian fake antifascist Facebook group
Threatened to remove Sam Houston statue in Hermann Park
Right-wing counter group (“This is Texas”) organized a rally in “defense”

https://www.thedailybeast.com/texas-conservatives-fall-for-anti-antifa-hoax
https://thinkprogress.org/hermann-park-protest-houston-28895d563f38/
Study by Morten Bay, **USC Annenberg School**

Collected 1273 tweets mentioning the film’s director
- 973 unique accounts after cleanup, deduplication
- Manually analyzed the sentiment of each tweet
- Manually categorized each tweeting account
- Also used Indiana U.’s “Botometer”

**Results?**
- 22% of accounts were negative
- 44 bot accounts, 61 “political” users
- 101 “fans” who were negative on the film

An academic paper finds that half of criticism aimed at director Rian Johnson was politically motivated.

Did *Star Wars: The Last Jedi* destroy the franchise and permanently rupture the fandom as its critics (melodramatically) have accused it of doing? According to a new academic paper by researcher Morten Bay, the answer is clearly no.

The paper, titled *Weaponizing The Haters: The Last Jedi and the Battle for Star Wars*, is the first in a series of studies examining social media activity related to films in the *Star Wars* franchise.
Study by Morten Bay, USC Annenberg School

Collected 1273 tweets mentioning Star Wars: The Last Jedi

- 973 unique accounts analyzed
- Manually analyzed the tweets
- Manually categorized each tweet
- Also used Indiana U.'s "Botometer"

Results?

- 22% of accounts were bots
- 44 bot accounts, 61 "political" users
- 101 "fans" who were negative on the film

"Russian trolls weaponize Star Wars criticism as an instrument of information warfare with the purpose of pushing for political change, while it is weaponized by right-wing fans to forward a conservative agenda and for some it is a pushback against what they perceive as a feminist/social justice onslaught."

Academic paper finds that half of the negative tweets were politically motivated.

Did Star Wars: The Last Jedi destroy the franchise and permanently rupture the fandom as its critics (melodramatically) have accused it of doing? According to a new academic paper by researcher Morten Bay, the answer is clearly no.

The paper, titled Weaponizing The Haters: The Last Jedi and its Fans, is available here.
Social networks respond
Social networks respond

‘Russian bots’ outcry: Is Twitter cracking down on people who challenge the status quo?

It seems that the bots (especially the ‘Russian bots’) narrative is being used as a kind of defensive mechanism, journalist and human rights activist Mike Raddie told RT amid reports of a massive account purge on Twitter.

A crackdown on bot spam or disinformation?

“The whole meme of the bots, especially the ‘Russian bots,’ is actually being used as a kind of defensive mechanism,” said Mike Raddie. “Whenever people criticize the corporate media in the West – we’ve done it with the Guardian – they come back and say, ‘oh, you’re sort of a Russian bot army,’ or a typical question is, ‘what’s the weather like in St. Petersburg? Is it amazing in Moscow yet?’ So it’s a very useful meme for corporate journalists to deflect any kind of criticism, especially over hot topics such as Syria, Ukraine – things like this.”

A number of Twitter accounts are said to have been flagged over the past few days, in what many have speculated is part of the company’s efforts to clamp down on the much-touted army of Russian-controlled automated accounts, or “bots.” However, Twitter has yet to elaborate on the reported mass purge, which allegedly also targeted users with right-wing views – raising concerns of political censorship on the popular social media platform. The hashtag #Twitter Contractors began trending on the site shortly after the suspensions.

‘Russian Today, Feb. 2018’

© Richard James Mendosa / Global Look Press

See what's happening in the world right now.
Twitter is sweeping out fake accounts like never before, putting user growth at risk

Twitter suspended more than 70 million accounts in May and June, and the pace has continued in July

By Craig Timberg and Elizabeth Dwoskin
July 6

SAN FRANCISCO — Twitter has sharply escalated its battle against fake and suspicious accounts, suspending more than 1 million a day in recent months, a major shift to lessen the flow of disinformation on the platform, according to data obtained by The Washington Post.

The rate of account suspensions, which Twitter confirmed to The Post, has more than doubled since October, when the company revealed under congressional pressure how Russia used fake accounts to interfere in the U.S. presidential election. Twitter suspended more than 70 million accounts in May and June, and the pace has continued in July, according to the data.

The aggressive removal of unwanted accounts may result in a rare decline in the number of monthly users in the second quarter, which ended June 30, according to a person familiar with the situation who was not authorized to speak. Twitter declined to comment on a possible decline in

Twitter is sweeping out fake accounts like never before, putting user growth at risk

Twitter suspended more than 70 million accounts in May and June, and the pace has continued in July

By Craig Timberg and Elizabeth Dwoskin
July 6

SAN FRANCISCO — Twitter has sharply escalated its battle against fake and suspicious accounts, suspending more than 1 million a day in recent months, a major shift to lessen the flow of disinformation on the platform, according to data obtained by The Washington Post.

The rate of account suspensions, which Twitter confirmed to The Post, has more than doubled since October, when the company revealed under congressional pressure how Russia used fake accounts to interfere in the U.S. presidential election. Twitter suspended more than 70 million accounts in May and June, and the pace has continued in July, according to the data.

The aggressive removal of unwanted accounts may result in a rare decline in the number of monthly users in the second quarter, which ended June 30, according to a person familiar with the situation who was not authorized to speak. Twitter declined to comment on a possible decline in daily users.
Social media summary

HOW RUSSIA HELPED SWING THE ELECTION FOR TRUMP

A meticulous analysis of online activity during the 2016 campaign makes a powerful case that targeted cyberattacks by hackers and trolls were decisive.

By Jane Mayer

https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump
Joel Benenson, the Clinton pollster, was stunned when he learned, from the July indictment, that the Russians had stolen his campaign's internal modelling. "I saw it and said, 'Holy shit!'" he told me. Among the proprietary information that the Russian hackers could have obtained, he said, was campaign data showing that, late in the summer of 2016, in battleground states such as Michigan, Wisconsin, and Pennsylvania, an unusually high proportion of residents whose demographic and voting profiles identified them as likely Democrats were "Hillary defectors": people so unhappy with Clinton that they were considering voting for a third-party candidate. The Clinton campaign had a plan for winning back these voters. Benenson explained that any Clinton opponent who stole this data would surely have realized that the best way to counter the plan was to bombard those voters with negative information about Clinton. "All they need to do is keep that person where they are," he said, which is far easier than persuading a voter to switch candidates. Many critics have accused Clinton of taking Michigan and Wisconsin for granted and spending virtually no time there. But Benenson said that, if a covert social-media campaign targeting "Hillary defectors" was indeed launched in battleground states, it might well have changed the outcome of the election.
Social media summary

Joel Benenson, the Clinton pollster, was stunned when he learned, from the July indictment, that the Russians had stolen his campaign's internal modelling. "I saw it and said, 'Holy shit!' " he told me. Among the proprietary information that the Russian hackers could have obtained, he said, was campaign data showing that, late in the summer of 2016, in battleground states such as Michigan, Wisconsin, and Pennsylvania, an unusually high proportion of residents whose demographic and voting profiles identified them as likely Democrats were "Hillary defectors": people so unhappy with Clinton that they were considering voting for a third-party candidate. The Clinton campaign had a plan for winning back these voters. Benenson explained that any Clinton opponent who stole this data would surely have realized that the best way to counter the plan was to bombard those voters with negative information about Clinton. "All they need to do is keep that person where they are," he said, which is far easier than persuading a voter to switch candidates. Many critics have accused Clinton of taking Michigan and Wisconsin for granted and spending virtually no time there. But Benenson said that, if a covert social-media campaign targeting "Hillary defectors" was indeed launched in battleground states, it might well have changed the outcome of the election.
So, how did the 2018 election go?
Military response!

US Cyber Command attacked Russian troll farm on Election Day 2018

‘Preventing this interference is one of our highest priorities,’ said US agencies at the time

By Russell Brandom | Feb 26, 2019, 2:07pm EST

The United States Cyber Command launched an offensive campaign to silence one of Russia’s most notorious troll operations on the day of the 2018 midterm elections, according to a new report by The Washington Post. The operation targeted the Internet Research Agency, a private company linked to the Kremlin and often used for disinformation campaigns.
Some U.S. officials argued that “grand strategic deterrence” is not always the goal. “Part of our objective is to throw a little curveball, inject a little friction, sow confusion,” said one defense official. “There’s value in that. We showed what’s in the realm of the possible. It’s not the old way of doing business anymore.”

The action has been hailed as a success by Pentagon officials, and some senators credited Cyber Command with averting Russian interference in the midterms.

“The fact that the 2018 election process moved forward without successful Russian intervention was not a coincidence,” said Sen. Mike Rounds (R-S.D.), who did not discuss the specific details of the operation targeting the St. Petersburg group. Without Cybercom’s efforts, he said, there “would have been some very serious cyber-incursions.”
How well defended are the voting machines, themselves?
California Top to Bottom Review (2007)

End of election inventory management / auditing

Attacked by voter
Viral attack vulnerabilities (Hart InterCivic)

California Top to Bottom Review (2007)

SERVO

End of election inventory management / auditing

Attacked by voter
Viral attack vulnerabilities (Hart InterCivic)

California Top to Bottom Review (2007)

End of election inventory management / auditing

SERVO

Attacked by voter
Viral attack vulnerabilities (Hart InterCivic)

California Top to Bottom Review (2007)

SERVO

End of election inventory management / auditing

Exploit

Attacked by voter
Viral attack vulnerabilities (Hart InterCivic)

California Top to Bottom Review (2007)

SERVO

Exploit

Attacked by voter

End of election inventory management / auditing
Viral attack vulnerabilities (Hart InterCivic)

California Top to Bottom Review (2007)

Exploit

End of election inventory management / auditing

Attacked by voter

All subsequent machines compromised.
Post-2016 improvements

Better “cyber-hygiene” for election officials, political campaigns
Example: Growing use of “two factor authentication”
EI-ISAC: Election Infrastructure Information Sharing and Analysis Center
  • A direct consequence of the DHS “critical infrastructure” designation
  • Federal assistance to states and counties

Some federal funds to improve security
But not enough to replace existing equipment

Summary: Better than nothing.
Can Dead Hackers Vote Twice? — Defcon Voting Village report: Bug in one system could “flip Electoral College”.

High-speed... A voting machine is submitted to abuse in DEFCON’s Voting Village. Sean Gallagher

SEAN GALLAGHER

DEF CON Voting Village Report Calls for Standards & Fixes

BY RYAN BOYER

Half of US states using voting machines with a known vulnerability, says report

The security flaw was flagged in 2007.

By Marianna Herman / September 27, 2015 11:42 AM PT

Defcon Voting Village Report: Bug in one system could "flip Electoral College"
California's voting makeover: All 58 counties race to update voting systems by 2020

Most California counties think they will make the deadline to update their voting systems, but 10 are requesting exemptions or extensions.

May 29, 2019, 1:06 PM CDT

By Kevin Monahan, Cynthia McFadden and Adiel Kaplan

SANTA ANA, Calif. – A sprawling warehouse on South Grand Avenue holds the 11,000 voting machines that Orange County, California – the nation's fifth-largest voting district – has used in its elections for the past two decades. Every single one of them is about to become scrap metal, thanks in part to the stroke of a state official's pen.

California Secretary of State Alex Padilla has long been concerned about the vulnerability of the nation's voting machines. "We have done more to respond to hanging chads," he told NBC News, "than we have done to respond to Vladimir Putin and the threats by Russian intelligence officials against our elections."
The problem is not unique to California, as states across the country scramble to deal with outdated voting technology before 2020. A study by the Brennan Center for Justice shows that **38 states use discontinued voting machines** — machines that are no longer manufactured — in one or more jurisdictions. Another seven states use voting machines that have been discontinued in every jurisdiction. That means only five states don't use at least some machines that are no longer manufactured.

By Kevin Monahan, Cynthia McFadden and Adiel Kaplan

SANTA ANA, Calif. — A sprawling warehouse on South Grand Avenue holds the 11,000 voting machines that Orange County, California — the nation's fifth-largest voting district — has used in its elections for the past two decades. Every single one of them is about to become scrap metal, thanks in part to the stroke of a state official's pen.

California Secretary of State Alex Padilla has long been concerned about the vulnerability of the nation's voting machines. "We have done more to respond to hanging chads," he told NBC News, "than we have done to respond to Vladimir Putin and the threats by Russian intelligence officials against our elections."
I know, let’s vote on the Internet!
The pitch: Convenience, turnout, cost

Similar arguments in favor of vote-by-mail
Vote from the convenience of your home!
We can do banking on the Internet! Why not voting?
We’ll just use blockchain, that will solve it!
The pitch: Convenience, turnout, cost

Similar arguments in favor of vote-by-mail

Vote from the convenience of your home!
We can do banking on the Internet! Why not voting?
We’ll just use *blockchain*, that will solve it!
Issue #0: Not everybody has a computer

You’re making voting more accessible to some people, but not others

Source: A Comparative Assessment of Electronic Voting (Feb. 2010), Canada-Europe Transatlantic Dialog
http://www.elections.ca/res/rec/tech/ivote/comp/ivote_e.pdf
Issue #0: Not everybody has a computer

You’re making voting more accessible to some people, but not others

Case studies of prior Internet / phone voting pilot projects.

Issue #1: Local coercion

Also an issue with vote-by-mail: you’re not in a secure polling place

No requirement for voter anonymity

Allows for bribery, coercion, retribution

Cracking Down on Mail-in Ballot Fraud

The Issue

Mail-in ballot fraud is “the tool of choice for those who are engaging in election fraud.”

Once seen only used when voters knew they were going to be out of town on Election Day, mail-in ballots have become commonplace in Texas and around the nation. The advent of early ended. Election law prohibits a polling place staffed by paid agents of one candidate or one political party, yet, ballot harvesters are functionally the same in many key respects as election judges.

The Facts

- Texas first allowed absentee voting in 1917; voting by mail
Issue #2: Your computer is insecure

1-2% of U.S. computers have malware on them. Maybe much more.
## Issue #2a: Older computers are worse

<table>
<thead>
<tr>
<th>Version</th>
<th>Codename</th>
<th>API</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.3-2.3.7</td>
<td>Gingerbread</td>
<td>10</td>
<td>0.3%</td>
</tr>
<tr>
<td>4.0.3-4.0.4</td>
<td>Ice Cream Sandwich</td>
<td>15</td>
<td>0.3%</td>
</tr>
<tr>
<td>4.1.x</td>
<td>Jelly Bean</td>
<td>16</td>
<td>1.2%</td>
</tr>
<tr>
<td>4.2.x</td>
<td></td>
<td>17</td>
<td>1.5%</td>
</tr>
<tr>
<td>4.3</td>
<td></td>
<td>18</td>
<td>0.5%</td>
</tr>
<tr>
<td>4.4</td>
<td>KitKat</td>
<td>19</td>
<td>6.9%</td>
</tr>
<tr>
<td>5.0</td>
<td>Lollipop</td>
<td>21</td>
<td>3.0%</td>
</tr>
<tr>
<td>5.1</td>
<td></td>
<td>22</td>
<td>11.5%</td>
</tr>
<tr>
<td>6.0</td>
<td>Marshmallow</td>
<td>23</td>
<td>16.9%</td>
</tr>
<tr>
<td>7.0</td>
<td>Nougat</td>
<td>24</td>
<td>11.4%</td>
</tr>
<tr>
<td>7.1</td>
<td></td>
<td>25</td>
<td>7.8%</td>
</tr>
<tr>
<td>8.0</td>
<td>Oreo</td>
<td>26</td>
<td>12.9%</td>
</tr>
<tr>
<td>8.1</td>
<td></td>
<td>27</td>
<td>15.4%</td>
</tr>
<tr>
<td>9</td>
<td>Pie</td>
<td>28</td>
<td>10.4%</td>
</tr>
</tbody>
</table>

Data collected during a 7-day period ending on May 7, 2019. Any versions with less than 0.1% distribution are not shown.
**Issue #2a: Older computers are worse**

Obsolete Android versions with dangerous security holes (3.8%).

Android versions which support newer security features (e.g., "hardware attestation") that would be useful (57.9%).

---

**Data collected during a 7-day period ending on May 7, 2019**

Any versions with less than 0.1% distribution are not shown.
Attackers could do “denial of service” attacks against election officials

Knock servers offline, unable to receive votes

The Russians (allegedly) did this to Estonia in 2007

A 2014 independent study found many more issues

https://estoniaevoting.org/
Many vendors get even the basics wrong (here, encryption settings)

- **Internet Voting for Persons with Disabilities - Security Assessments of Vendor Proposals** (2014)
- Commissioned by the City of Toronto


Of the three vendors, Dominion had the best SSL/TLS server configuration:

- **Scytl’s grade**: B (source: SSL Labs Grade for demo.scytl.com). Scytl’s server gets a mediocre score for its TLS configuration. Issues include: not supporting TLS 1.1 or 1.2; allowing the use of weak key lengths (via 56-bit DES); and for not explicitly preferring stronger connections over DES. Scytl’s server also supports TLS compression, a known vulnerability. While the server supports cipher modes that provide forward secrecy, it does not explicitly prefer them. Scytl’s use of client-side encryption may moot this point if the client-side encryption uses a semantically secure (randomized) encryption algorithm (though we were not able to confirm it).

- **Dominion’s grade**: A (source: SSL Labs Grade for intvoting.com). Dominion’s server gets a strong score for its TLS configuration. It supports TLS 1.2 and only offers encryption with at least 128 bits. It is not perfect as it prefers RC4, which mitigates BEAST, but has its own vulnerabilities (see the Traffic Analysis section below), and it does not offer forward secrecy at all.

- **Everyone Counts’ grade**: B (source: SSL Labs Grade for elect.everyonecounts.com). Everyone Counts’ server gets a mediocre score for its TLS configuration. It support TLS 1.2, prefers to use strong 256-bit encryption, but does support weak (56 bit) DES encryption. It does not explicitly mitigate BEAST server-side. It offers and prefers forward secrecy.

We note again that the grading scheme is not our own, and it is designed for general purpose HTTPS configurations, however we believe it is a useful benchmark to establishing the degree to which the vendors comply with best practices.
Issue #4: The election server is insecure

Many vendors get even the basics wrong (here, encryption settings)

- Internet Voting for Persons with Disabilities - Security Assessments of Vendor Proposals (2014)
- Commissioned by the City of Toronto


Of the proposals evaluated in the context of the [Toronto, Canada] RFP process, it is our opinion that no proposal provides adequate protection against the risks inherent in internet voting. It is our recommendation, therefore, that the City not proceed with internet voting in the upcoming municipal election. If the City, contrary to this recommendation, remains committed to the use of internet voting, we advise that the system be limited to voters with disabilities, and not offered to the electorate at large.

Of the three vendors, Dominion had the best SSL/TLS server configuration:

- Scytl's grade: B (source: SSL Labs Grade for demo.scytl.com). Scytl's server gets a mediocre score for its TLS configuration. Issues include: not supporting TLS 1.1 or 1.2; allowing the use of weak key lengths (via 56-bit DES); and for not explicitly preferring stronger connections over DES. Scytl's server also supports TLS compression, a known vulnerability. While the server supports cipher modes that provide forward secrecy, it does not explicitly prefer them. Scytl's use of client-side encryption may moot this point if the client-side encryption uses a semantically secure (randomized) encryption algorithm (though we were not able to confirm it).

- Dominion's grade: A (source: SSL Labs Grade for intvoting.com). Dominion's server gets a strong score for its TLS configuration. It supports TLS 1.2 and only offers encryption with at least 128 bits. It is not perfect as it prefers RC4, which mitigates BEAST, but has its own vulnerabilities (see the Traffic Analyses section below), and it does not offer forward secrecy at all.

- Everyone Counts' grade: B (source: SSL Labs Grade for elect.everyonecounts.com). Everyone Counts' server gets a mediocre score for its TLS configuration. It supports TLS 1.2, prefers to use strong 256-bit encryption, but does support weak (56-bit) DES encryption. It does not explicitly mitigate BEAST server-side. It offers and prefers forward secrecy.

We note again that the grading scheme is not our own, and it is designed for general purpose HTTPS configurations, however we believe it is a useful benchmark to establishing the degree to which the vendors comply with best practices.
Many vendors get even the basics wrong (here, encryption settings):

- Internet Protocol
- Asynchronous Transfer Mode
- Computer Network
- Toronto

From the Estonian study (2014):

Assistant Professor J. Alex Halderman ... pointed to fundamental weaknesses in the I-voting system's design. “Estonia’s Internet voting system blindly trusts the election servers and the voters’ computers”, Halderman said. “Either of these would be an attractive target for state-level attackers, such as Russia.” Recent reports about state-sponsored hacking of American companies by China and European telecoms by the NSA demonstrate that these dangers are a reality, Halderman explained.

Of the three vendors, Dominion had the best SSL/TLS server configuration:

- Of the proposals evaluated in the context of the [Toronto, Canada] RFP process, it is our opinion that no proposal provides adequate protection against the risks inherent in internet voting. It is our recommendation, therefore, that the City not proceed with internet voting in the upcoming municipal election. If the City, contrary to this recommendation, remains committed to the use of internet voting, we advise that the system be limited to voters with disabilities, and not offered to the electorate at large.

We note again that the grading system is not perfect, and it is designed for general purposes. HTTPS configurations, however we believe it is a useful benchmark to establishing the degree to which the vendors comply with best practices.
Issue #5: Secure schemes are unusable

Code voting: you mail the voter a paper, mapping candidates $\rightarrow$ codes
Client computer malware doesn’t know the codes, can’t switch candidates
If it tells you the verification code, you know the remote server saw it!

Estimate the usability of this scheme:

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Voting Code</th>
<th>Verification Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>KGHW</td>
<td>PSDN</td>
</tr>
<tr>
<td>Bob</td>
<td>DKFO</td>
<td>SDFQ</td>
</tr>
<tr>
<td>Charlie</td>
<td>WCAS</td>
<td>LFOC</td>
</tr>
<tr>
<td>Dorothy</td>
<td>DGTO</td>
<td>QXSZ</td>
</tr>
</tbody>
</table>
### Issue #5: Secure schemes are unusable

**Code voting:** you mail the voter a paper, mapping *candidates* → *codes*

Client computer malware doesn’t know the codes, can’t switch candidates.
If it tells you the verification code, you know the remote server saw it!

**Estimate the usability of this scheme:**

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Voting Code</th>
<th>Verification Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>KGHW</td>
<td>PSDN</td>
</tr>
<tr>
<td>Bob</td>
<td>DKFO</td>
<td>SDFQ</td>
</tr>
<tr>
<td>Charlie</td>
<td>WCAS</td>
<td>LFOC</td>
</tr>
<tr>
<td>Dorothy</td>
<td>DGTO</td>
<td>QXSZ</td>
</tr>
</tbody>
</table>
Companies make claims that their tech cannot possibly support...
Companies make claims that their tech can:

- Leveraging blockchain and cybersecurity that surpasses even most government standards, we'll enable you to vote from practically anywhere in the world from your favorite mobile device. (Or would you rather wait in line at the polling station?)

- Our CastIron™ Mobile Blockchain Voting Platform – is verifiable from end-to-end and built from the ground up to serve the needs of our dedicated elections teams. You'll be proud to work with an election system that verifiably accurate knowing that every vote was counted as intended.
Companies make claims that their tech cannot possibly support

There are no government standards here to exceed.

Meaningless claims without proof.

Leveraging blockchain and cybersecurity that surpasses even most government standards, we'll enable you to vote from practically anywhere in the world from your favorite mobile device. (Or would you rather wait in line at the polling station?)

Our CastIron™ Mobile Blockchain Voting Platform – is verifiable from end-to-end and built from the ground up to serve the needs of our dedicated elections teams. You'll be proud to work with an election system that verifiably accurate knowing that every vote was counted as intended.
Fundamental cryptographic errors
The implementation of the commitment scheme in the SwissPost-Scyt\l
mixnet uses a trapdoor commitment scheme, which allows an authority who
knows the trapdoor values to generate a shuffle proof transcript that passes
verification but actually alters votes. We give two examples of details of how
this could be used. The first example allows the first mix to use the trapdoors
to substitute votes for which it knows the randomness used to generate the
encrypted vote. The second example does not even require knowledge of the
random factors used to generate the votes, and could be used by the last mix
in the sequence.

---

Since making this work public, we have learned that the same issue was identified independently
by Thomas Raine of NTNU, and also by Rolf Haenni of the Bern University of Applied Sciences,
https://e-voting.bfh.ch/publications/2019/
The implementation of the commitment scheme in the SwissPost-Scytl mixnet uses a trapdoor commitment scheme, which allows an authority who knows the trapdoor values to generate a shufffle proof transcript that passes verification but actually alters votes. We give two examples of details of how this could be used. The first example allows the first mix to use the trapdoors to substitute votes for which it knows the randomness used to generate the encrypted vote. The second example does not even require knowledge of the random factors used to generate the votes, and could be used by the last mix in the sequence.

Since making this work public, we have learned that the same issue was identified independently by Thomas Haines of NTNU, and also by Rolf Haenni of the Bern University of Applied Sciences, https://e-voting.bfh.ch/publications/2019/
Fundamental cryptographic errors

The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system

Sarah Jamie Lewis¹, Olivier Pereira², and Vanessa Teague³

¹Open Privacy Research Society, sarah@openprivacy.ca
²UCLouvain – ICTeam, B-1348 Louvain-la-Neuve, Belgium, olivier.pereira@uclouvain.be
³The University of Melbourne, Parkville, Australia, vjteague@unimelb.edu.au

March 12, 2019

The implementation of the commitment scheme in the SwissPost-Scytl mixnet uses a trapdoor commitment scheme, which allows an authority who knows the trapdoor values to generate a shuffel proof transcript that passes verification but actually alters votes. We give two examples of details of how this could be used. The first example allows the first mix to use the trapdoors to substitute votes for which it knows the randomness used to generate the encrypted vote. The second example does not even require knowledge of the random factors used to generate the votes, and could be used by the last mix in the sequence.

---

Swiss Post Public Intrusion Test

Undetectable Attack Against Vote Integrity and Secrecy

ROLF HAENNI

Bern University of Applied Sciences

1 Theoretical Background

Commitment schemes are usually perfectly binding and computationally hiding. This means that no information about the message can be derived from the commitment and that the commitment can not be opened to a message other than the original one. The Pedersen commitment scheme achieves these properties by computing \( c = G^{m} H^{r} \) in a multiplicative cyclic group, for which the discrete logarithm assumption (DL) is believed to hold. This scheme is perfectly binding, because a randomization \( r' \neq r \) exists for any other message \( m' \neq m \) such that \( c = G^{m} H^{r} \). This means that \( c \) could potentially be open to all \( q \) messages from \( Z_{q} \), but this requires the computation of the discrete logarithm. The Swiss Post voting protocol works with a subgroup \( G_{q} \subseteq Z_{q} \) of integers modulo \( q \), where \( q = |G_{q}| \) denotes the prime order of the subgroup, \( m \in Z_{q} \) the message, and \( r \in Z_{q} \) the randomization. Both \( G \) and \( H \) are elements of \( G_{q} \).

A pre-condition for the scheme to be computationally binding is the independence of the two values \( G, H \in G_{q} \setminus \{1\} \) [in a group of prime order \( q \), both values are generators of \( G_{q} \)]. Independence means that respective discrete logarithms \( b = \log_{G} H \) and \( g = \log_{G} G \) are unknown to everyone. Otherwise, for example if \( h = \log_{G} H \) is known to the person who created \( c \), then \( c \) can be rewritten as

\[ c = G^{m} H^{r} = G^{m'r} = G^{hr \mod q}. \]

Therefore, to open \( c \) to a different message \( m' \neq m \), the adversary can easily solve

\[ m + hr \equiv m' + hr' \pmod{q}. \]

to find the matching randomization \( r' = (m - m')h^{-1} + r \mod q \). As a consequence, the binding property of the commitment scheme is completely broken in that case.

---

*Since making this work public, we have learned that the same issue was identified independently by Thomas Ruane of NTNU, and also by Rolf Haenni of the Bern University of Applied Sciences, https://e-voting.bfh.ch/publications/2019/*
Internet voting summary

No.
The current debate in the U.S.: Hand-marked paper ballots vs. machine-marked paper ballots
Hand-marked paper

Nice security properties
No computers between voter and the record of their vote intent

Usability limitations
Huge, multi-page ballots

Ambiguous marks
Require officials to intuit the “intent of the voter”
Hand-marked paper

Nice security properties
No computers between voter and the record of their vote intent

Usability limitations
Huge, multi-page ballots

Ambiguous marks
Require officials to intuit the “intent of the voter”

Famous example: “Lizard people” ballot, Coleman vs. Franken (MN Senate race, 2008)
Risk limiting audits

Random sampling of individual paper ballots
Each should exactly match up with electronic records
Required in many states, growing in popularity
  • Requires touching tens of ballots, rarely hundreds, unlikely more

Mitigates malicious software in the ballot scanners
Discrepancies require more samples, degenerates to a full manual recount of the ballots
Machine-marked paper

Bad engineering decisions
Barcode scanner vs. text OCR
Malicious software could change barcodes, voter will never know

But includes essential features
Can easily support thousands of ballot styles (essential for “vote centers”)
Button boxes, headphones, etc.

Open question: risk-limiting audits
Machine-marked paper

Bad engineering decisions
Barcode scanner vs. text OCR
Malicious software could change barcodes, voter will never know

But includes essential features
Can easily support thousands of ballot styles (essential for “vote centers”)
Button boxes, headphones, etc.

Open question: risk-limiting audits
Bad engineering decisions
Barcode scanner vs. text OCR
Malicious software could change barcodes, voter will never know

But includes essential features
Can easily support thousands of ballot styles (essential for “vote centers”) Button boxes, headphones, etc.

Open question: risk-limiting audits
Better engineering: Los Angeles VSAP

Large touchscreen, integrated ballot box, plain paper ballots
Voters can see the ballot, aren’t required to touch it
But can an evil machine still print one thing while a voter doesn’t notice?
STAR-Vote (Travis County + academics)

Touch-screen user interface
Prints a human-readable paper ballot

E2e cryptography
Rapid, verifiable tallies

Risk-limiting audits

Procurement process ultimately failed
STAR-Vote (Travis County + academics)

Touch-screen user interface
Prints a human-readable paper ballot

E2e cryptography
Rapid, verifiable tallies

Risk-limiting audits

Procurement process ultimately failed

Rice prototype STAR-Vote ballot scanner
Microsoft's open 'ElectionGuard' SDK aims to secure democratic elections

ElectionGuard is open source and built to make sure votes are verifiable, secure, and auditable.
To encrypt a ballot, you encrypt each position separately

Additive homomorphism:

\[ E_k(A + B) = E_k(A) \oplus E_k(B) \]

- No voter can decrypt their vote
- Every voter can recompute the encrypted total
- Every voter can verify their encrypted vote was included in the tally
Crypto coolness 1: NIZK proofs

Every encrypted counter has a proof that it's either zero or one
No way for “ballot stuffing” with huge ballots

Election officials also produce a “decryption proof” after the election
Any observer can see the encrypted ballots, validate the total
We can replace “the election official” with “a group of trustees”

Important cryptographic operations can be split across $n$ trustees, where $k$ of them must cooperate to perform the operation.

To an external observer, everything looks like a regular public key operation.

Trustees produce a proof (NIZK) that their result is correct.
Crypto coolness 3: hash chaining

Every ballot “receipt” includes a hash of the encrypted ballot
Voter can validate integrity of their (encrypted) ballot, but can’t prove plaintext

Every ballot receipt hash can also covers prior ballots (same precinct)
Mass ballot loss or tampering will be easily detected

Copies on every local machine
Lots of copies = lots of opportunity to discover problems

Similar ideas in crypto-currency “blockchains” but no reason to do consensus. Disagreements resolved after the election.
Catch a machine if it cheats!

Benaloh challenges [2006]
Catch a machine if it cheats!

Benaloh challenges [2006]

voter makes selections
Catch a machine if it cheats!

Benaloh challenges [2006]

voter makes selections

voting machine commits irrevocably to the ballot to be cast
Catch a machine if it cheats!

Benaloh challenges [2006]

voter makes selections

voting machine commits irrevocably to the ballot to be cast

"cast"

"challenge"

voter's choice
Catch a machine if it cheats!

Benaloh challenges [2006]

voter makes selections

voting machine commits irrevocably to the ballot to be cast

"cast"

voter's choice

"challenge"

confirmed (ballot is cast)
Catch a machine if it cheats!

Benaloh challenges [2006]

voter makes selections

voting machine commits irrevocably to the ballot to be cast

“cast”

voter’s choice

“challenge”

confirmed (ballot is cast)

show commitment (ballot is spoiled)
Post-election verification

Separate page to take home
Ballot hash for lookup on “public bulletin board”

Cast ballot: ciphertext will match
Challenge ballot: plaintext also present, verifiable
Vote tallying: provably includes all ballots on the bulletin board
Hash chains: also publicly verifiable
How not to do e2e cryptography
How not to do e2e cryptography

Ceci n’est pas une preuve
The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system

Sarah Jamie Lewis¹, Olivier Pereira², and Vanessa Teague³

¹Open Privacy Research Society, sarah@openprivacy.ca
²UCLouvain – ICTeam, B-1348 Louvain-la-Neuve, Belgium, olivier.pereira@uclouvain.be
³The University of Melbourne, Parkville, Australia, vjteague@unimelb.edu.au

March 12, 2019

The implementation of the commitment scheme in the SwissPost-Scytl mixnet uses a trapdoor commitment scheme, which allows an authority who knows the trapdoor values to generate a shuffle proof transcript that passes verification but actually alters votes. We give two examples of details of how this could be used. The first example allows the first mix to use the trapdoors to substitute votes for which it knows the randomness used to generate the encrypted vote. The second example does not even require knowledge of the random factors used to generate the votes, and could be used by the last mix in the sequence.

Since making this work public, we have learned that the same issue was identified independently by Thomas Haines of NTNU, and also by Rolf Haenni of the Bern University of Applied Sciences, https://e-voting.bfh.ch/publications/2019/
How not to do e2e cryptography

The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system

Sarah Jamie Lewis¹, Olivier Pereira², and Vanessa Teague³

¹Open Privacy Research Society, sarah@openprivacy.ca
²UCLouvain – ICTeam, B-1348 Louvain-la-Neuve, Belgium, olivier.pereira@uclouvain.be
³The University of Melbourne, Parkville, Australia, vjteague@unimelb.edu.au

March 12, 2019

The implementation of the commitment scheme in the SwissPost-Scytl mixnet uses a trapdoor commitment scheme, which allows an authority who knows the trapdoor values to generate a shuffle proof transcript that passes verification but actually alters votes. We give two examples of details of how this could be used. The first example allows the first mix to use the trapdoors to substitute votes for which it knows the randomness used to generate the encrypted vote. The second example does not even require knowledge of the random factors used to generate the votes, and could be used by the last mix in the sequence.

Since making this work public, we have learned that the same issue was identified independently by Thomas Haines of NTNU, and also by Rolf Haenni of the Bern University of Applied Sciences, https://e-voting.bfh.ch/publications/2019/

1 Theoretical Background

Commitment schemes are usually perfectly hiding and computationally binding. This means that no information about the message can be derived from the commitment and that the commitment can not be opened to a message other than the original one. The Pedersen commitment scheme achieves these properties by computing $c = G^m H^r$ in a multiplicative cyclic group, for which the discrete logarithm assumption (DL) is believed to hold. This scheme is perfectly binding, because a randomization $r' \neq r$ exists for any other message $m' \neq m$ such that $c = G^{m'} H^{r'}$. This means that $c$ could potentially be opened to all $q$ messages from $\mathbb{Z}_q$, but this requires the computation of the discrete logarithm. The Swiss Post voting protocol works with a subgroup $G_q \triangleq \mathbb{Z}_p^*$ of integers modulo $p$, where $q = |G_q|$ denotes the prime order of the subgroup, $m \in \mathbb{Z}_q$ the message, and $r \in \mathbb{Z}_q$ the randomization. Both $G$ and $H$ are elements of $G_q$.

A pre-condition for the scheme to be computationally binding is the independence of the two values $G, H \in G_q \setminus \{1\}$ (in a group of prime order $q$, both values are generators of $G_q$). Independence means that respective discrete logarithms $h = \log_G H$ and $g = \log_H G$ are unknown to everyone. Otherwise, for example if $h = \log_G H$ is known to the person who created $c$, then $c$ can be rewritten as

$$c = G^m H^{r'} = G^{m'} (G^r)^{r'} = G^{m' + r r' \mod q}.$$ 

Therefore, to open $c$ to a different message $m' \neq m$, the adversary can easily solve

$$m + hr \equiv m' + hr' \pmod{q}$$

to find the matching randomization $r' = (m - m') h^{-1} + r \mod q$. As a consequence, the binding property of the commitment scheme is completely broken in that case.
The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system

Sarah Jamie Lewis1, Olivier Pereira2, and Vanessa Teague3

1Open Privacy Research Society, sarah@openprivacy.ca
2UCLouvain – ICTeam, B-1348 Louvain-la-Neuve, Belgium, olivier.pereira@uclouvain.be
3The University of Melbourne, Parkville, Australia, vjteague@unimelb.edu.au

March 12, 2019

The implementation of the commitment scheme in the SwissPost-Scytl mixnet uses a trapdoor commitment scheme, which allows an authority who knows the trapdoor values to generate a shuffle proof transcript that passes verification but actually alters votes. We give two examples of details of how mixnet uses a trapdoor commitment scheme, which allows an authority who

Ap r e - c o n d i t i o n f o r t h e s c h e m e t o b e c o m p u t a t i o n a l l y b i n d i n g i s t h e

Logarithm. The Swiss Post voting protocol works with a subgroup $G$ of the multiplicative cyclic group, for which the discrete logarithm assumption (DL) is believed to hold. This scheme is perfectly hiding, because a randomization $r^*$ exists for any other message $m^* \neq m$ such that $c = G^{\log H}$.

Commitment schemes are usually perfectly hiding and computationally binding. This means that no information about the message can be derived from the commitment and that the commitment can not be opened to a message other than the original one. The Pedersen commitment scheme achieves these properties by computing $c = G^{\log H}$ in a multiplicative cyclic group, for which the discrete logarithm assumption (DL) is believed to hold. This scheme is perfectly hiding, because a randomization $r^*$ exists for any other message $m^* \neq m$ such that $c = G^{\log H}$. This means that $c$ could potentially be opened to all $m$ messages from $Z_q$, but this requires the computation of the discrete logarithm. The Swiss Post voting protocol works with a subgroup $G \leq Z_q$ of integers modulo $q$, where $q = |G|$ denotes the prime order of the subgroup, $m \in Z_q$ the message, and $r \in Z_q$ the randomization. Both $G$ and $r$ are elements of $G_q$.

A pre-condition for the scheme to be computationally binding is the independence of the two values $G, H \in G_q \setminus \{1\}$. Independence means that respective discrete logarithms $b = \log_G H$ and $g = \log_q G$ are unknown to everyone. Otherwise, for example if $H = \log_b G$ is known to the person who created $c$, then $c$ can be rewritten as $c = G^{\log H} = G^{b \cdot G^h} = G^{b \cdot G^h \mod q}$. Therefore, to open $c$ to a different message $m^* \neq m$, the adversary can easily solve $m + hr \equiv m^* + hr^* \pmod q$ to find the matching randomization $r^* = (m - m^*)/h^{-1} + r \mod q$. As a consequence, the binding property of the commitment scheme is completely broken in that case.

1 Theoretical Background

The Swiss Post Public Intrusion Test

Undetectable Attack Against Vote Integrity and Secrecy

ROLF HAENNI

Bern University of Applied Sciences

1. Swiss Post Public Intrusion Test

Online Democracy

Swiss Post’s e-voting system pulled for May votes

MAR 29, 2019 - 13:46

Swiss Post’s e-voting system had been in use in four cantons: Basel City, Fribourg, Neuchâtel and Thurgau.

The e-voting system operated by Swiss Post will not be available for nationwide votes on May 19. This is the consequence of “critical errors” found during a public intrusion test, the Federal Chancellery and Swiss Post announced on Friday.

The Federal Chancellery of swissinfo in a statement it would review the licensing and certification procedures for e-voting systems. It added that it had no indication that these flaws had resulted in votes being manipulated in previous ballots.

Swiss Post’s e-voting system had been in use in four cantons: Basel City, Fribourg, Neuchâtel and Thurgau.

Since making this work public, we have learned that the same issue was identified independently by Thomas Ramee of NTNU, and also by Rolf Haenni of the Bern University of Applied Sciences, https://evoting.ber.ch/publications/2019/
Will ElectionGuard be better?

Talented engineers & researchers from Microsoft Research and Galois
Both organizations have important expertise with software correctness
  • Theorem provers, model checkers, static analyses, etc.
  • Galois is building a prototype similar to STAR-Vote

The ElectionGuard model: open-source, verified libraries
Targeted outreach to election equipment vendors

Still requires in-precinct voting
Sophisticated cryptography doesn’t solve problems with internet voting
Are we ready for the 2020 U.S. election?

Voter registration data is probably still vulnerable
Growing importance of early voting and election-day vote centers
These databases must be online to check off voters as they sign in!

End-to-end schemes are (sadly) still years away from production

Internet voting schemes are a really bad idea
Acknowledgements

ACCURATE - A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections
NSF research center on e-voting, 2005-2011
Many ideas in STAR were developed in ACCURATE

NSF: Voting Systems Architectures for Security and Usability
Research support for STAR effort, 2014-2018

Microsoft SEIF
Investigating integration of Win10 measured boot (2013)