The Ballot is Busted Before the Blockchain:
A Security Analysis of Voatz, the First Internet Application used in U.S. Federal Elections

specter@mit.edu
Michael A. Specter, James Koppel, Danny Weitzner

In February, the state of West Virginia abruptly abandoned plans to adopt an internet voting phone app called Voatz

This research is why.

WEST VIRGINIA LEGISLATURE

2020 REGULAR SESSION

Enrolled
Committee Substitute
for
Senate Bill 94

SENATORS TRUMP, WELD, AZINGER, BALDWIN, BEACH, CLEMENTS, CLINE, HARDESTY, JEFFRIES, LINDSAY, MAYNARD, PITSENBARGER, ROMANO, RUCKER, SMITH, TAKUBO, WOELFEL, HAMILTON, STOLLINGS, IHLENFELD, AND SYPOLT, *original sponsors*

[Passed January 24, 2020; in effect from passage]

AN ACT to amend and reenact §3-3-1, §3-3-2, §3-3-2b, §3-3-4, §3-3-5, and §3-3-6 of the Code of West Virginia, 1931, as amended; and to amend said code by adding thereto a new section, designated §3-3-1a, all relating generally to absentee voting; clarifying that voters with disabilities prevented from voting in person may vote by mail-in absentee ballot; providing that voters with physical disabilities may vote by electronic absentee ballot; clarifying that certain overseas military members and citizens may vote by electronic absentee ballot; defining terms; providing that a voter with a physical disability may electronically submit an application to

22%

of adults in WV with “Serious Difficulty Walking or Climbing Stairs”- CDC (https://www.cdc.gov/ncbddd/disabilityandhealth/impacts/west-virginia.html)

Voatz

Questions

- Does Voatz provide the essential security requirements of voting?
  - Correctness: Counted as cast, cast as intended, usability
  - Privacy: An attacker cannot learn a voter's selections
  - Receipt Freeness: No voter can prove the way they voted
  - Coercion Resistance: A voter cannot cooperate with an attacker to prove the way they voted
- Advertised use of cryptography:
  - Hardware-backed key storage!
  - Mixnets!
  - And, of course, the Blockchain!
  - Is this End to end verifiable (E2E-V)?

Methodology

- Challenge:
  - Can’t touch server infrastructure (legal & ethical concerns)
  - Must make assumptions about the backend
- Solution:
  - Manually reverse engineer the Voatz Android app
  - Iteratively reimplement the server to understand protocol
  - For analysis, assume the best possible situation for the backend

Results

- 5 high-severity vulnerabilities & a serious privacy issue
- Many basic implementation failures, e.g.:
  - Mandated use of weak passwords
  - Anti-tamper/AV solution was easily circumventable
  - Sends a photo of user's ID, and location to a third party *without alerting the user*
- API Server has complete control
  - No proofs of inclusion (where's the Blockchain?)
  - Weak receipt validation, not E2E-V

Adversary	**Attacker Capability**				
	Suppress Ballot	Learn Secret Vote	Alter Ballot	Learn User's Identity	Learn User IP
Passive Network (§5.3)		✓			✓
Active Network (§5.3)	✓	✓			✓
3rd-Party ID Svc. (§5.4)	✓			✓	✓
Root On-Device (§5.1)	✓	✓	✓	✓	✓
Voatz API Server (§5.2)	✓	✓	✓	✓	✓

Example:
Passive Network Attack

Voatz

Standard HTTPS

Gen 100 ECDSA Key Pairs.
Discards all secret keys,
except #57

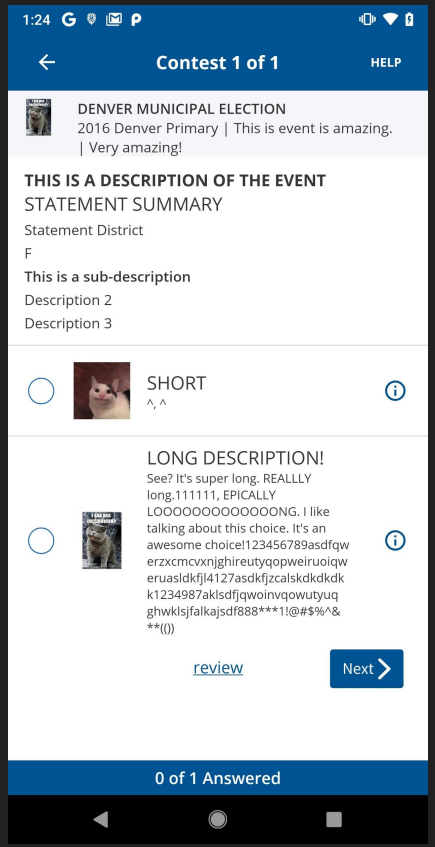
100 ECDSA Pubkeys

Gen 100 ECDSA key pairs
Key_{57} ← Key agreement
with the sender's 57th key
$AESGCM_{sk}$ ←$ R

$ECDSA_{Enc}(Key_{57}, AESGCM_{sk})$, 100 PubKeys

Perform key agreement &
decrypt $AESGCM_{sk}$

All comms $Enc(AESGCM_{sk}, *)$




```
Short_Candidate = {
    "choiceDetails" :   {
        "imageUrl": short.com/img.jpg,
        "webUrl"  : short.com/desc
    },
    "choiceId": "1",
    "description": "Short",
    "description 1": "^",
    "description 2": "^",
    "isWriteIn":  False,
    "nonSelectable" : False
}

Long_Candidate = {
    "choiceDetails": {
        "imageUrl": www.LONG_IMG_URL.info/LONG_IMG_URL.jpg,
        "webUrl"  : www.LONG_IMG_URL.info/Long_Candidate_Info
    },
    "choiceId" : "2",
    "description": "Long Description !",
    "description 1" : "See? It's super long .REALLLY long.111111",
    "description 2" : "EPICALLYLOOOOOOOOOOOOONG....",
    "isWriteIn":  False ,
    "nonSelectable" : False
}
```

When the user submits their ballot

- Sends *all* metadata of the voter's choice
- But only that candidate's metadata

```
Short_Candidate = {
    "choiceDetails" :   {
        "imageUrl": short.com/img.jpg,
        "webUrl"  : short.com/desc
    },
    "choiceId": "1",
    "description": "Short",
    "description 1": "^",
    "description 2": "^",
    "isWriteIn":  False,
    "nonSelectable" : False
}

Long_Candidate = {
    "choiceDetails": {
        "imageUrl": www.LONG_IMG_URL.info/LONG_IMG_URL.jpg,
        "webUrl"  : www.LONG_IMG_URL.info/Long_Candidate_Info
    },
    "choiceId" : "2",
    "description": "Long Description !",
    "description 1" : "See? It's super long .REALLLY
long.111111",
    "description 2" : "EPICALLYLOOOOOOOOOOOOONG....",
    "isWriteIn":  False ,
    "nonSelectable" : False
}
```

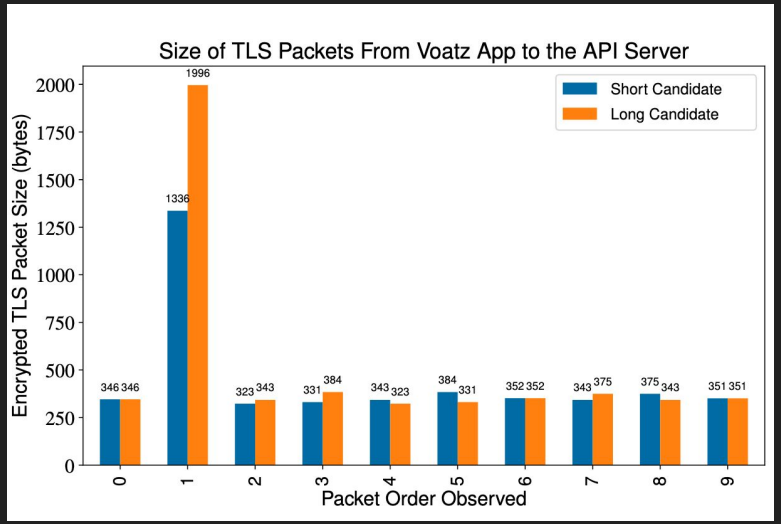
Textbook Side-channel attack

Regular HTTPS:

- Ciphertext = AES(gzip(data))
- len(ciphertext) ~= len(gzip(data))
- Plaintext length is *somewhat* obfuscated

Voatz Protocol:

- Ciphertext = AES(gzip(AES(data))
- len(gzip(AES(data))) = len(data)
- len(Ciphertext) ~= len(data)



How did this happen?

Obfuscation.

Documentation

- FAQ with a bunch of security claims (https://perma.cc/FBQ8-N875)
  - No formal description of their system
- No security reviews made public
- No list of fixed vulns
- Unclear claims
  - “...doubly anonymized: first by the smartphone, and second by the blockchain server network.”
  - “...end-to-end vote encryption and vetting the certificates represented by unique IDs stored on the smartphone …”
  - “anonymized voter-verified digital receipts”
  - “ voter-verified audit trail”

Code Obfuscation

- All code was obfuscated using Proguard
- Protocol strings (e.g. “AES_GCM”) were obfuscated
  - Used a string-encoding scheme that deobfuscated at run-time
  - Common in games, DRM kits, and malware
- Nonstandard 57th key protocol
- “Bug bounty” version of the app also obfuscated
- No concrete security benefit
  - ...but it does make independent analysis harder.

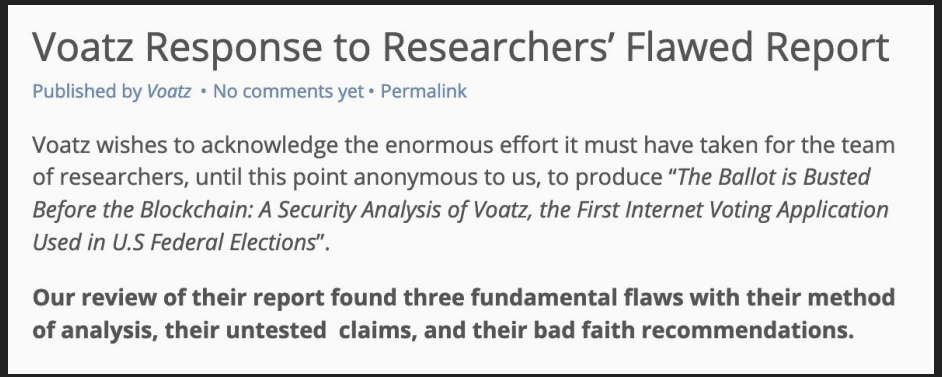
“We fully support the West Virginia Secretary of State’s office and the law enforcement agencies in their investigations under the purview of the law. Given that our elections infrastructure is classified as critical infrastructure under the Department of Homeland Security, we will continue to report any such attempts in the future.”

- CEO Nimit Sawhney

https://statescoop.com/voatz-voting-app-west-virginia-fbi-hacking-attempt/

OK, then.


U.S. DEPARTMENT OF HOMELAND SECURITY
CISA
CYBER+INFRASTRUCTURE



Voatz Response to Researchers' Flawed Report

Published by *Voatz* • No comments yet • Permalink

Voatz wishes to acknowledge the enormous effort it must have taken for the team of researchers, until this point anonymous to us, to produce "*The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S Federal Elections*".

Our review of their report found three fundamental flaws with their method of analysis, their untested claims, and their bad faith recommendations.

"...the researchers' true aim is to deliberately disrupt the election process, to sow doubt in the security of our election infrastructure, and to spread fear and confusion."

https://blog.voatz.com/?p=1243

Voatz

"...the researchers were analyzing an Android version of the Voatz mobile voting app that was at least 27 versions old at the time of their disclosure and not used in an election."

"...the researchers fabricated an imagined version of the Voatz servers, hypothesized how they worked, and then made assumptions about the interactions between the system components that are simply false."

https://blog.voatz.com/?p=1243

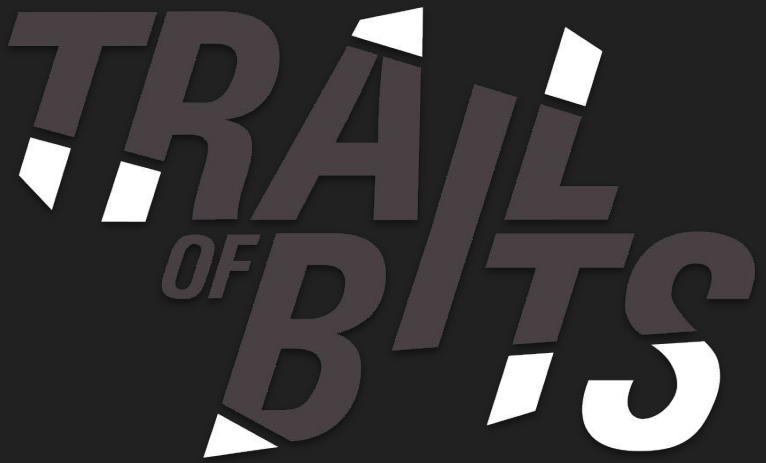
"The unit has security software that was two generations old, and to our knowledge is not used anywhere in the country."

"By any standard – academic or common sense – the study is unrealistic and inaccurate."

https://freedom-to-tinker.com/2006/09/20/refuting-diebolds-response/

Voatz's own 3rd Party Security Analysis

- Confirmed vulns in most recent version
- Confirmed severity
  - *Before Voatz spoke to the press*
- Validated our methodology
- Found many server-side issues:
  - AV wasn't running during past elections
  - +40 other issues
- ...Still not an *independent* audit



hackerone

“We partner with organizations that prioritize acting in good faith towards the security researcher community and providing adequate access to researchers for testing.

Because the Voatz program did not adhere to either of those requirements, we terminated our partnership in March 2020.”

Conclusions.

It’s not that the cybersecurity people are bad people, per se.

I think it’s that they are solving for one situation, and I am solving for another. They want zero technology risk in any way, shape, or form. [...] I am solving for the problem of turnout.

-Bradley Tusk, Voatz Backer & Mobile Voting Project founder

Argument:
Solve a Policy Problem through Technology

Problem: Unanalyzed Risk.

Asymmetric Information

Recommendations

1. Fight efforts to increase information asymmetry.

2. Universal public scrutiny of deployed elections systems.

3. Uphold standards of software independence, verifiability, & transparency in elections systems.

Hack on everything else.

specter@mit.edu

Michael A. Specter, James Koppel, Danny Weitzner