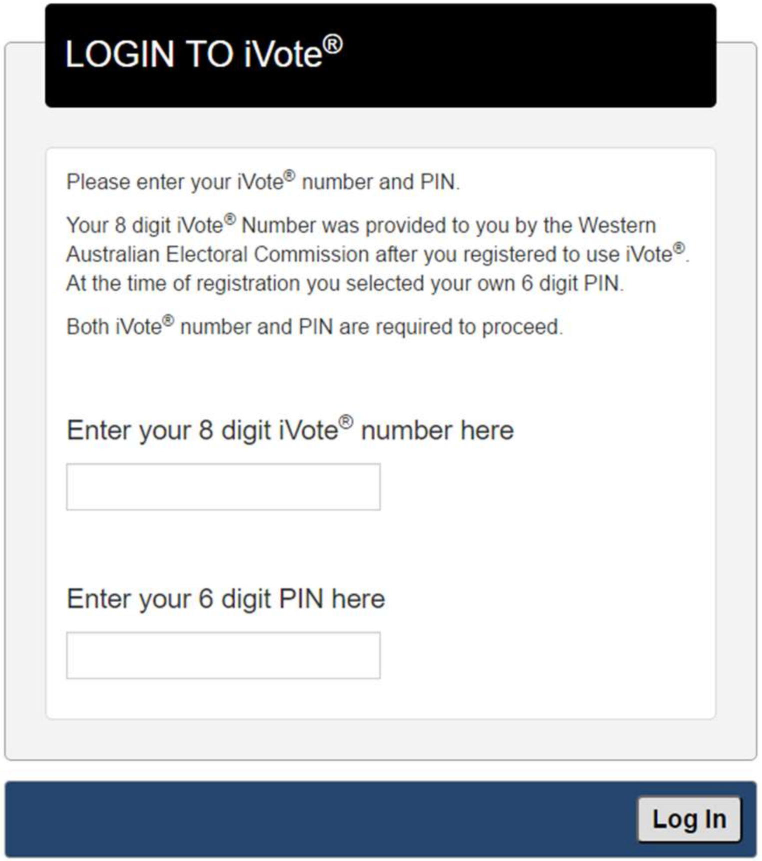
iVote®

Online Voting and DDoS Mitigation

The Story of iVote WA 2017

Mark Eldridge



LOGIN TO iVote®

Please enter your iVote® number and PIN.

Your 8 digit iVote® Number was provided to you by the Western Australian Electoral Commission after you registered to use iVote®. At the time of registration you selected your own 6 digit PIN.

Both iVote® number and PIN are required to proceed.

Enter your 8 digit iVote® number here

Enter your 6 digit PIN here

BACKGROUND

Elections and trust

Modern democratic governance is built upon a foundation of free and fair elections.

- Trust in the election process requires that election systems are both fair, and seen to be fair.

“Elections serve two purposes. First, and most obvious, they are how we choose a winner.

“But second, and equally important, they convince the loser—and all the supporters—that he or she lost.”

- Bruce Schneier[1]

To preserve this trust, the result of an election must accurately reflect the will of the voters.

- Trust in institutions has decreased in recent years
- Younger voters are less likely to trust election outcomes

[1] Schneier, Bruce. 2016. “American Elections Will Be Hacked”

[2] Karp et. al. The Australian Voter Experience: Trust and confidence in the 2016 federal election. Department of Government and International Relations, University of Sydney, 2017.

BACKGROUND

Trustworthy systems

In computer security:

- A **trusted** system is one we rely upon for our security model
- A **trustworthy** system is one which can be proven to be worthy of that trust

Our election systems are *trusted*, but are they trust*worthy*?

How do we prove the trustworthiness of an election system?

- Is our proof accessible to the average voter - i.e. will they trust the proof?
- Paper-based voting systems are easily understood by voters

BACKGROUND

Design of election systems

A well-designed voting system requires four features:

Accuracy	Reflect the intent of voters
Tamper Resistance	Protect against any individual or group attempting to manipulate the outcome
Privacy and Anonymity	Prevent a voter’s identity from being connected with their vote
Accessibility	Provide all voters with a vote and an understanding of the voting process

Voting systems can involve compromises between these features

- Postal votes and assisted voting (provides **accessibility** at the expense of **privacy and anonymity**)

BACKGROUND

Voting: a unique security problem

Elections present a unique security and privacy problem:

1. We must accurately identify voters, to ensure they vote only once.
2. Voter privacy must be protected, even from the voting system itself

Online voting is not like online banking

If an *online banking system* is compromised, we can compare what happened (money gone) to what we expected (money still here)

If an *online voting system* is compromised, there’s no counterfactual.

BACKGROUND

How does online voting work?

The electronic equivalent of the postal vote

Voters can vote anywhere from a personal device, usually over the internet

- Introduces a new risk: compromised devices

Multiple jurisdictions use online voting:

- Estonia
- Switzerland
- Australia
  - Trial for ADF personnel (via DRN, 2007)
  - iVote (NSW, WA)

Estonian e-ID card and reader

BACKGROUND

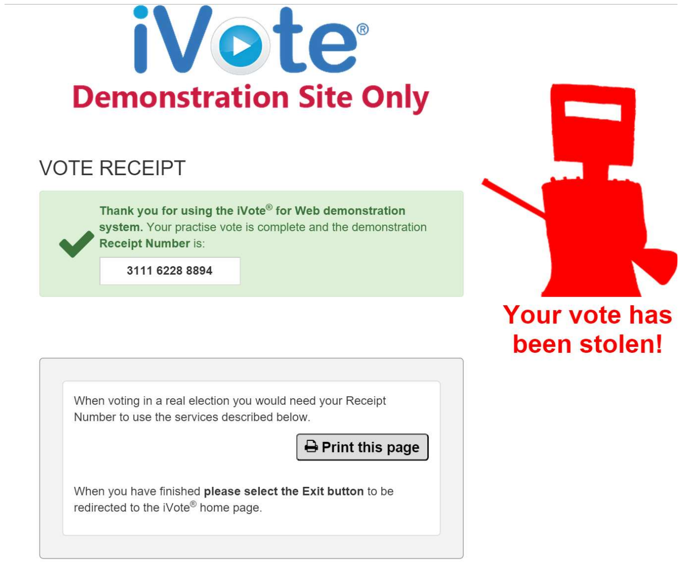
iVote NSW (2015)

The iVote online voting system

- Developed by Scytl Secure Electronic Voting
- First used in Australia for the 2015 NSW State Election
- The largest ever binding election to use online voting (280,000 votes)
- Included a telephone verification service where voters could have their completed ballot read back to them

Serious flaws identified in Transport Layer Security used by iVote

- The iVote website loaded third-party scripts over a weak TLS connection
- A man-in-the-middle-attacker could inject malicious scripts to read or modify completed ballots
- Telephone verification service also allowed for coercion attacks on voters



iVote®
Demonstration Site Only

VOTE RECEIPT

Thank you for using the iVote® for Web demonstration system. Your practise vote is complete and the demonstration **Receipt Number** is:

3111 6228 8894

When voting in a real election you would need your Receipt Number to use the services described below.

When you have finished **please select the Exit button** to be redirected to the iVote® home page.

Your vote has been stolen!

J. Alex Halderman, and Vanessa Teague. 2015. “The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election.”

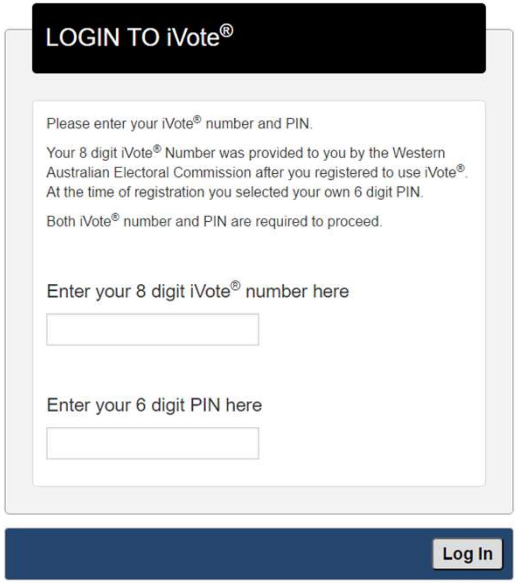
iVote WA: The 2017 WA State Election

iVote was also used for the 2017 WA state election

- The same system as used in NSW in 2015 (same server)
- All voter connections were proxied through a cloud-based CDN

Analysis of iVote WA performed February – May 2017

- Dr Chris Culnane and Dr Vanessa Teague (University of Melbourne)
- Dr Aleksander Essex (University of Western Ontario)
- Paper presented at Second Joint International Conference on Electronic Voting (E-Vote-ID), in Bregenz, Austria



LOGIN TO iVote®

Please enter your iVote® number and PIN.

Your 8 digit iVote® Number was provided to you by the Western Australian Electoral Commission after you registered to use iVote®. At the time of registration you selected your own 6 digit PIN.

Both iVote® number and PIN are required to proceed.

Enter your 8 digit iVote® number here

Enter your 6 digit PIN here

Chris Culnane, Mark Eldridge, Aleksander Essex, and Vanessa Teague. Trust Implications of DDoS Protection in Online Elections. In Electronic Voting, Lecture Notes in Computer Science, pages 127–145. Springer, Cham, October 2017.

THE IVOTE WA ONLINE VOTING SYSTEM

The iVote WA Voting Process

iVote is advertised as an end-to-end encrypted voting system

- The voter logs into the system using a pre-shared registration number and PIN
- Connections between the voter and the iVote server are encrypted using Transport Layer Security (TLS)
- Encryption of ballots is performed in the voter’s browser using JavaScript
- On completion of voting, voters are provided a receipt number, for the telephone verification service

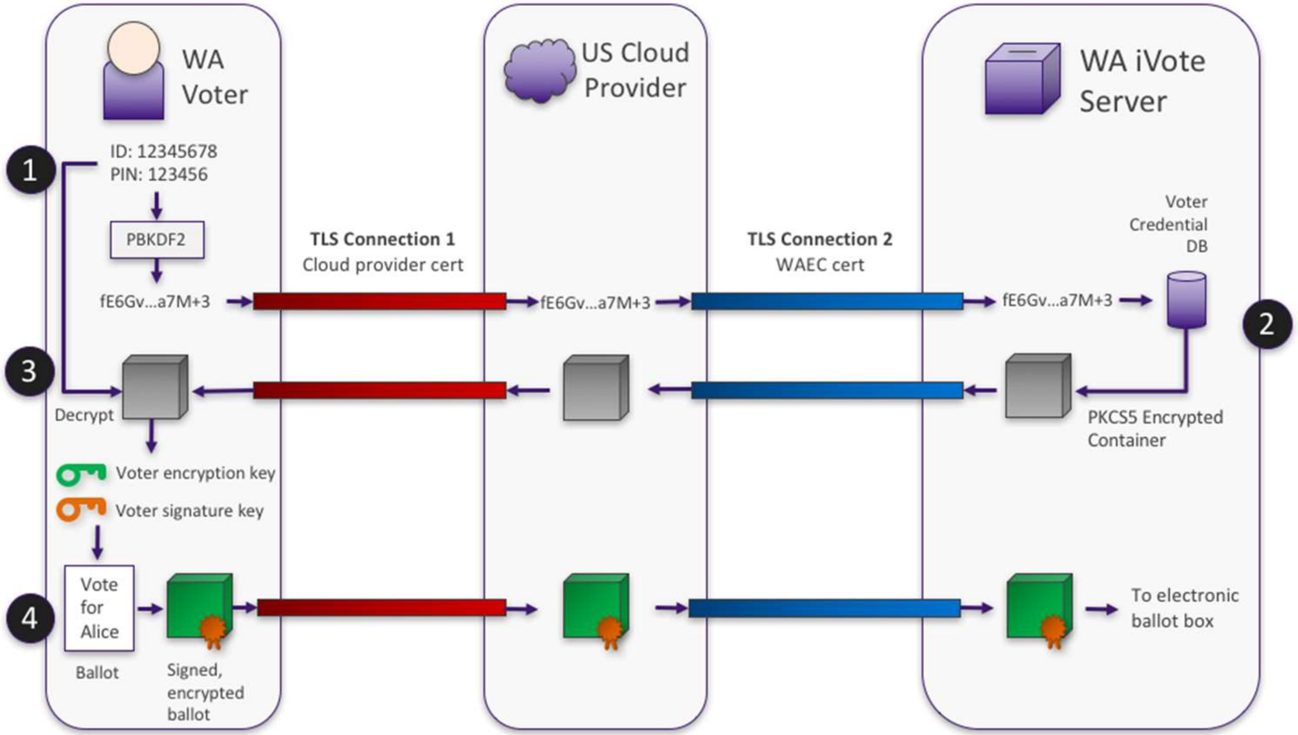
This security model assumes the encryption JavaScript is securely delivered to voters.

For iVote WA, the WA Electoral Commission (WAEC) purchased DDoS mitigation

- Imperva’s Incapsula service, a U.S. based Content Delivery Network (CDN)
- Relies upon Incapsula’s servers intercepting connections between voters and server (in plaintext)

The iVote WA Online Voting System

The iVote WA Voting Process



Essex, Aleksander. 2017. “iVote in Western Australia.” *Whisper Lab*. (https://whisperlab.org/blog/2017/iVote-in-Western-Australia.html)

THE iVOTE WA ONLINE VOTING SYSTEM

Incapsula and TLS Interception

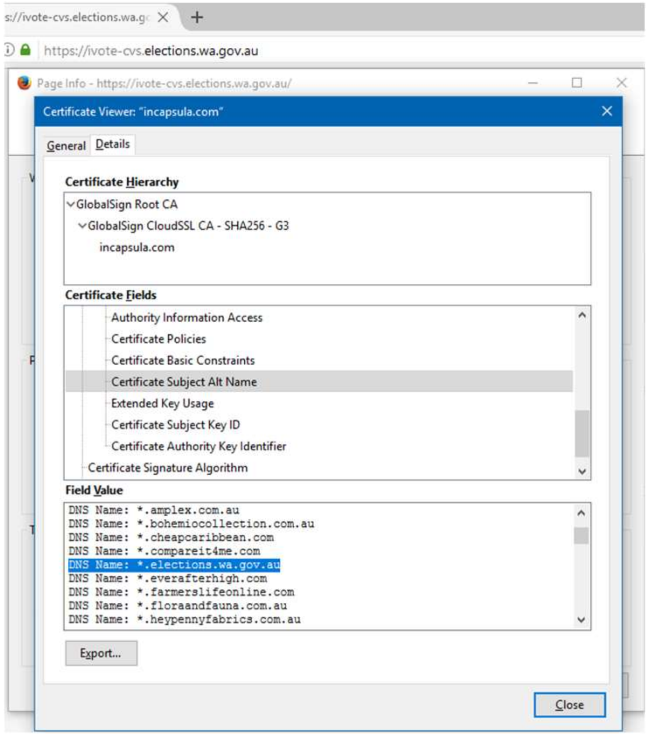
Incapsula acts as a reverse proxy for iVote

- Connections to `ivote-cvs.elections.wa.gov.au`
- Voter TLS connections terminate at Incapsula servers
- Decrypted connections are checked to determine whether they are legitimate users, and then forwarded to the iVote server

Voters see Incapsula's TLS certificate for `*.elections.wa.gov.au`

- Certificate shared with a number of other domains

This TLS certificate is stored at each Incapsula PoP


s://ivote-cvs.elections.wa.g
https://ivote-cvs.elections.wa.gov.au
Page Info - https://ivote-cvs.elections.wa.gov.au/
Certificate Viewer: "incapsula.com"
General
Details
Export...
Close

Certificate Hierarchy

- GlobalSign Root CA
  - GlobalSign CloudSSL CA - SHA256 - G3
    - incapsula.com

Certificate Fields

- Authority Information Access
- Certificate Policies
- Certificate Basic Constraints
- Certificate Subject Alt Name
- Extended Key Usage
- Certificate Subject Key ID
- Certificate Authority Key Identifier
- Certificate Signature Algorithm

Field Value

```
DNS Name: *.amplex.com.au
DNS Name: *.bohemiocollection.com.au
DNS Name: *.cheapcaribbean.com
DNS Name: *.compareit4me.com
DNS Name: *.elections.wa.gov.au
DNS Name: *.everafterhigh.com
DNS Name: *.farmerslifeonline.com
DNS Name: *.floraandfauna.com.au
DNS Name: *.heypennyfabrics.com.au
```

The Incapsula TLS certificate served by `107.154.128.220` (Melbourne PoP for `ivote-cvs.elections.wa.gov.au`)

The iVote WA Online Voting System

Incapsula JavaScript Injection

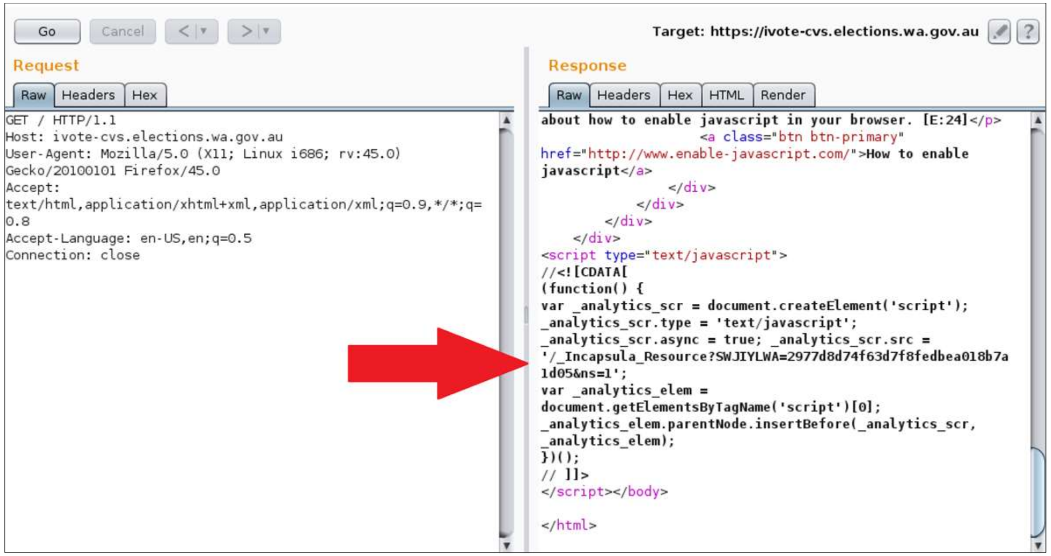
When Incapsula detects a new connection, the response from the iVote server is modified

The proxy injects obfuscated JavaScript

- Designed to fingerprint the user's device
- Includes basic browser fingerprinting techniques, as well as CPU and WebGL detection
- Result written into an Incapsula tracking cookie

This is common practice for DDoS mitigation

- Need to correctly identify legitimate traffic



```
GET / HTTP/1.1
Host: ivote-cvs.elections.wa.gov.au
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Connection: close
```

```
about how to enable javascript in your browser. [E:24]</p>
                    <a class="btn btn-primary"
href="http://www.enable-javascript.com/">How to enable
javascript</a>
                </div>
            </div>
        </div>
    </div>
<script type="text/javascript">
//<![CDATA[
(function() {
var _analytics_scr = document.createElement('script');
_analytics_scr.type = 'text/javascript';
_analytics_scr.async = true; _analytics_scr.src =
'/_Incapsula_Resource?SWJIYLWA=2977d8d74f63d7f8fedbea018b7a
1d05&ns=1';
var _analytics_elem =
document.getElementsByTagName('script')[0];
_analytics_elem.parentNode.insertBefore(_analytics_scr,
_analytics_elem);
})();
// ]]>
</script></body>

</html>
```

Herzberg, Ben, and Yoav Cohen. 2017. "How Incapsula Prevents Data Leaks." *Incapsula Blog*.

THE IVOTE WA ONLINE VOTING SYSTEM

JavaScript Injection: Security Implications

There is nothing malicious about Incapsula's JavaScript injection

- But for an online voting system like iVote, there are significant security implications
- The iVote security model assumes that TLS connections to the voter cannot be broken

What would happen if Incapsula's systems were compromised?

An attacker could modify the JavaScript injected by Incapsula:

- Passively snoop registration numbers and PINs, allowing decryption of ballots
- Actively modify ballots (impossible to detect from the server, unlikely to be detected by the voter)

These attacks would also be possible for any man-in-the-middle attacker with the TLS private key

THE iVOTE WA ONLINE VOTING SYSTEM

Foreign Hosting of TLS Private Keys

Incapsula's global network: 32 points of presence (PoPs)

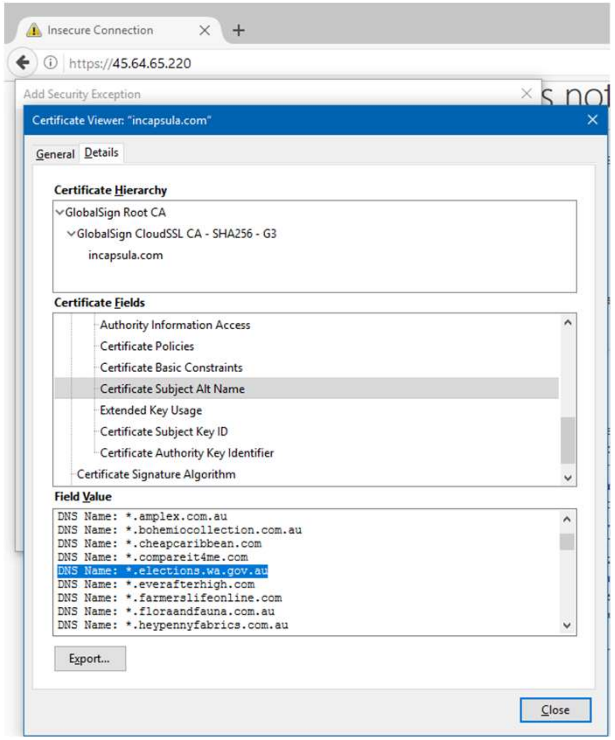
- The Americas, Europe, Middle East, and Asia Pacific

Certificates hosted in one PoP are propagated worldwide

- Ensures that user connections can be proxied by the closest PoP
- Also means the TLS private keys are propagated worldwide

Incapsula server in Hong Kong (`45.64.65.220`)

- Serves a valid TLS certificate for `*.elections.wa.gov.au`



Certificate Hierarchy

- GlobalSign Root CA
  - GlobalSign CloudSSL CA - SHA256 - G3
    - incapsula.com

Certificate Fields

- Authority Information Access
- Certificate Policies
- Certificate Basic Constraints
- Certificate Subject Alt Name
- Extended Key Usage
- Certificate Subject Key ID
- Certificate Authority Key Identifier
- Certificate Signature Algorithm

Field Value

```
DNS Name: *.amplex.com.au
DNS Name: *.bohemiocollection.com.au
DNS Name: *.cheapcaribbean.com
DNS Name: *.compareit4me.com
DNS Name: *.elections.wa.gov.au
DNS Name: *.everafterhigh.com
DNS Name: *.farmerslifeonline.com
DNS Name: *.floraandfauna.com.au
DNS Name: *.heypennyfabrics.com.au
```

The Incapsula TLS certificate served by `45.64.65.220`
(Hong Kong PoP for `ivote-cvs.elections.wa.gov.au`)

Incapsula Global Network Map: https://www.incapsula.com/incapsula-global-network-map.html.

THE IVOTE WA ONLINE VOTING SYSTEM

Foreign Hosting: Security Implications

Each Incapsula certificate has a SAN containing multiple domains

- The wildcard domain `*.elections.wa.gov.au` is one of many
- Other domains represent other Incapsula customers
- The private key for this certificate is located on multiple foreign PoPs

A foreign government, for legitimate domestic surveillance, may request the TLS private key for another Incapsula customer

- This customer could be listed in the same certificate SAN
- The foreign government could then perform man-in-the-middle attacks on connections to WA election infrastructure
- This includes the iVote Registration and Core Voting System (CVS)

```
X509v3 Subject Alternative Name:
DNS:incapsula.com,
DNS:*.1strongteam.com,
DNS:*.absolutewatches.com.au,
DNS:*.advancemotors.com.au,
DNS:*.alconchirurgia.pl,
DNS:*.amplex.com.au,
DNS:*.bohemiocollection.com.au,
DNS:*.cheapcaribbean.com,
DNS:*.compareit4me.com,
DNS:*.elections.wa.gov.au,
DNS:*.everafterhigh.com,
DNS:*.farmerslifeonline.com,
DNS:*.floraandfauna.com.au,
DNS:*.heypennyfabrics.com.au,
DNS:*.homeaway.com.ph,
DNS:*.jetblackespresso.com.au,
DNS:*.lifemapco.com,
DNS:*.lovemyearth.net,
DNS:*.maklernetz.at,
DNS:*.mobile-vertriebe.de,
DNS:*.mobile.zurich.com.ar,
...(continued)
```

THE iVOTE WA ONLINE VOTING SYSTEM

Clash Attacks on Voter Verification

The iVote system incorporates a telephone verification service for voters

- Voters dial a provided number, and enter their iVote ID, PIN, and receipt number
- Telephone verification service then reads back the completed ballot
- Intended to provide voters with a way to verify that their vote was not modified in any way

In 2015, Halderman & Teague identified several attacks against this system

- The “clash attack”: uses a previous (unmodified) vote as verification evidence for multiple voters
- Relies upon predicting a voter’s preferences at time of registration
- An attacker with access to Incapsula’s systems could perform more accurate clash attacks
- Incapsula tracking cookie applies across multiple websites, including iVote registration and voting

J. Alex Halderman, and Vanessa Teague. 2015. “The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election.”

The iVote WA Online Voting System

How not to implement DDoS mitgation

Incapsula’s DDoS mitigation relies upon DNS to reroute attacks

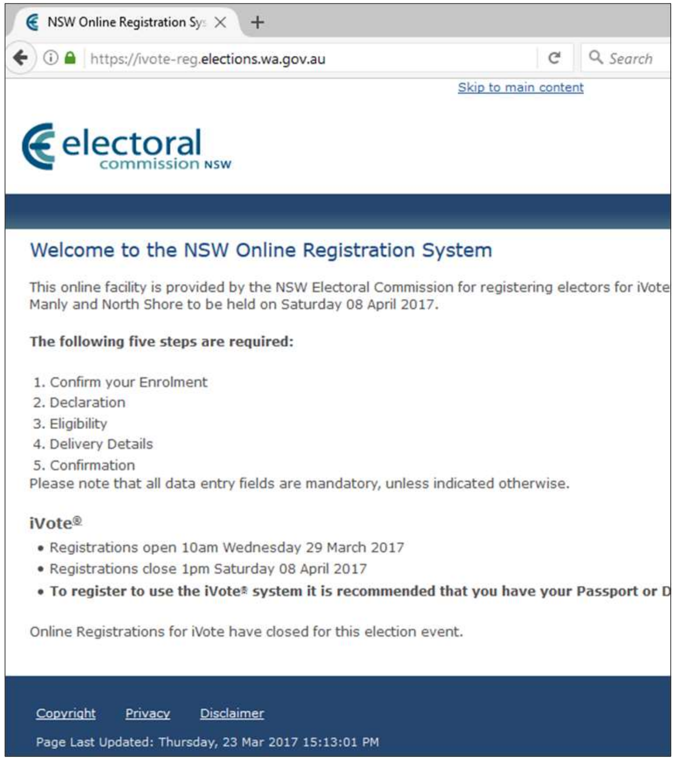
- Attackers targeting iVote infrastructure instead hit Incapsula

It is critical that the actual iVote infrastructure is hidden

- If attackers could find the IP address, they could DDoS it directly
- Normal practice is to block any connections from non-Incapsula IPs

This was not done for iVote WA

- Shared infrastructure with iVote NSW, and cached DNS entries
- Could perform direct-to-origin DDoS against the iVote CVS
- The WAEC was notified immediately, and mitigated the issue


NSW Online Registration Sy
https://ivote-reg.elections.wa.gov.au
Search
electoral commission NSW

Skip to main content

Welcome to the NSW Online Registration System

This online facility is provided by the NSW Electoral Commission for registering electors for iVote
Manly and North Shore to be held on Saturday 08 April 2017.

The following five steps are required:

1. Confirm your Enrolment
2. Declaration
3. Eligibility
4. Delivery Details
5. Confirmation

Please note that all data entry fields are mandatory, unless indicated otherwise.

iVote®

- Registrations open 10am Wednesday 29 March 2017
- Registrations close 1pm Saturday 08 April 2017
- **To register to use the iVote® system it is recommended that you have your Passport or D**

Online Registrations for iVote have closed for this election event.

Copyright Privacy Disclaimer

Page Last Updated: Thursday, 23 Mar 2017 15:13:01 PM

THE iVOTE WA ONLINE VOTING SYSTEM

The 2017 NSW By-Elections

Three by-elections were held in NSW on 8 April 2017

- Incapsula was used for registration and practise websites
- Incapsula did **not** cover the CVS (`cvs.ivote.nsw.gov.au`)

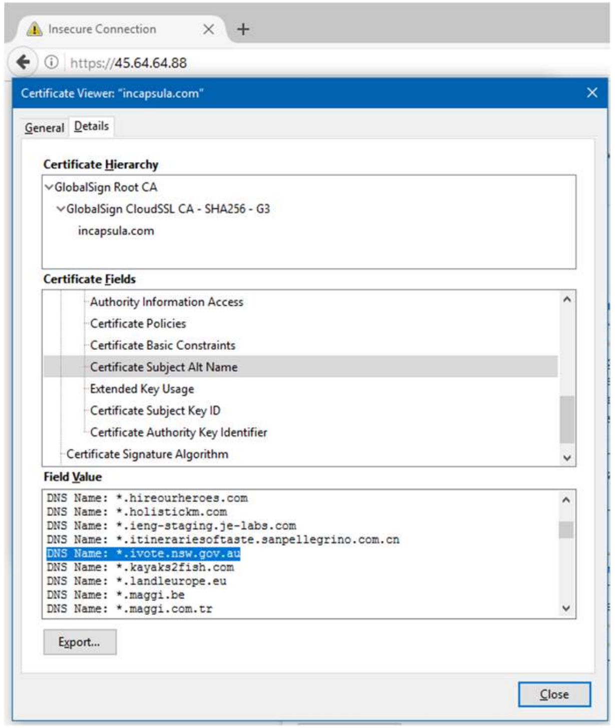
The Incapsula certificate is a wildcard `*.ivote.nsw.gov.au`

- As for iVote WA, this certificate is propagated worldwide

Incapsula server in Hong Kong (`45.64.64.88`)

- Serves a valid TLS certificate for `*.ivote.nsw.gov.au`

As before, this means a foreign government could demand access to a TLS private key covering iVote domains



Certificate Hierarchy

- GlobalSign Root CA
  - GlobalSign CloudSSL CA - SHA256 - G3
    - incapsula.com

Certificate Fields

- Authority Information Access
- Certificate Policies
- Certificate Basic Constraints
- Certificate Subject Alt Name
- Extended Key Usage
- Certificate Subject Key ID
- Certificate Authority Key Identifier
- Certificate Signature Algorithm

Field Value

```
DNS Name: *.hireourheroes.com
DNS Name: *.holistickm.com
DNS Name: *.ieng-staging.je-labs.com
DNS Name: *.itinerariesoftaste.sanpellegrino.com.cn
DNS Name: *.ivote.nsw.gov.au
DNS Name: *.kayaks2fish.com
DNS Name: *.landleurope.eu
DNS Name: *.maggi.be
DNS Name: *.maggi.com.tr
```

The Incapsula TLS certificate served by `45.64.64.88`
(Hong Kong PoP for `bypractise.ivote.nsw.gov.au`)

THE iVOTE WA ONLINE VOTING SYSTEM

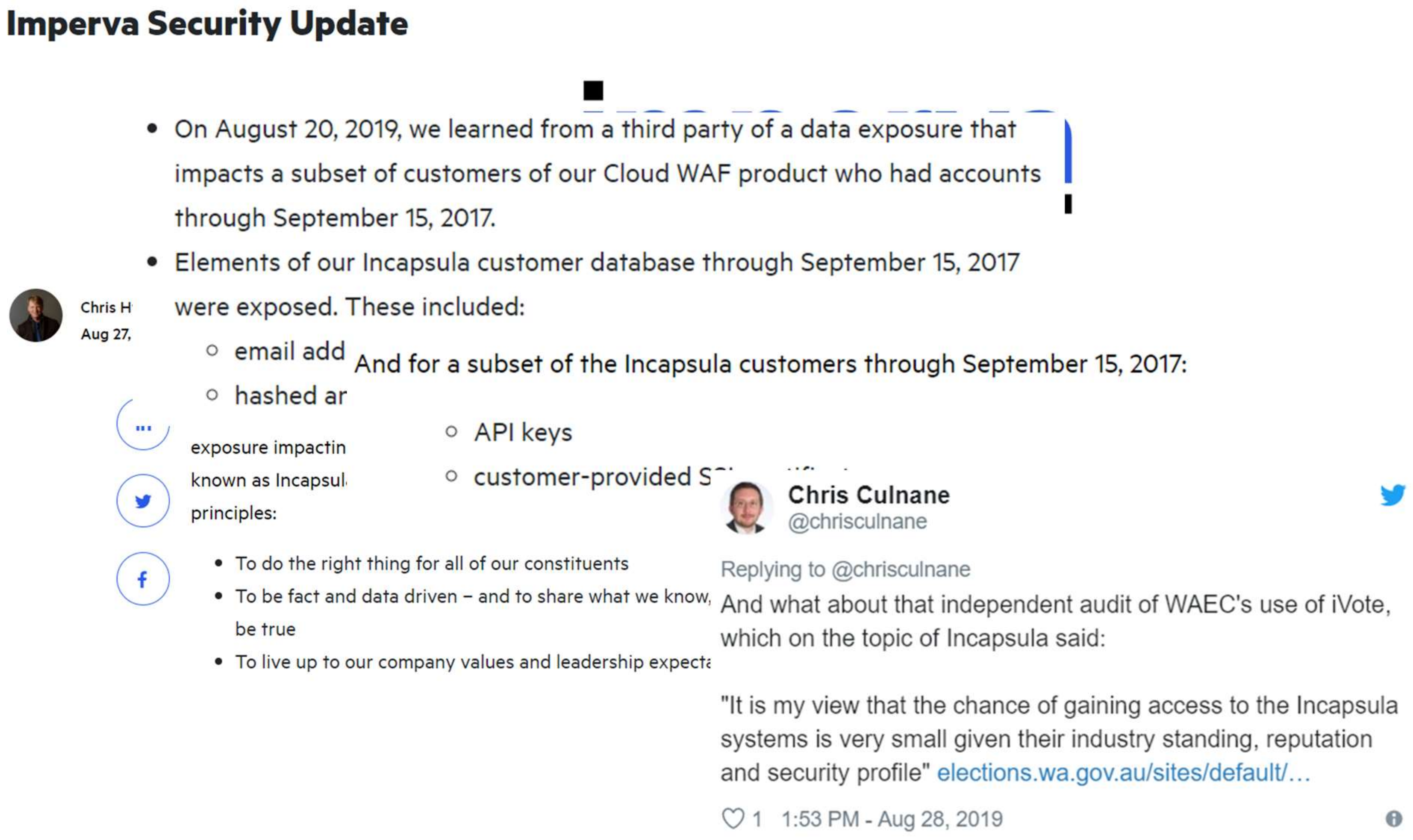
Summary

iVote WA used a cloud-based DDoS mitigation service (Incapsula)

- TLS proxying breaks the security assumptions for iVote’s ballot encryption
- Incapsula injects JavaScript into voter connections
- TLS private keys for iVote infrastructure are stored in foreign countries
- Use of Incapsula could allow more accurate clash attacks can be performed
- The DDoS mitigation was not implemented correctly, defeating the purpose

All voting systems involve trade-offs between usability, security, and voter perception

- Secure online voting is an incredibly hard problem
- Election officials need to understand these problems, and the trade-offs they are making
- Voters deserve full transparency about the security of their ballots



Imperva Security Update

- On August 20, 2019, we learned from a third party of a data exposure that impacts a subset of customers of our Cloud WAF product who had accounts through September 15, 2017.
- Elements of our Incapsula customer database through September 15, 2017 were exposed. These included:
  - email add
  - hashed ar

Chris H
Aug 27,

exposure impactin
known as Incapsul
principles:

- To do the right thing for all of our constituents
- To be fact and data driven – and to share what we know,
be true
- To live up to our company values and leadership expecta

And for a subset of the Incapsula customers through September 15, 2017:

- API keys
- customer-provided S

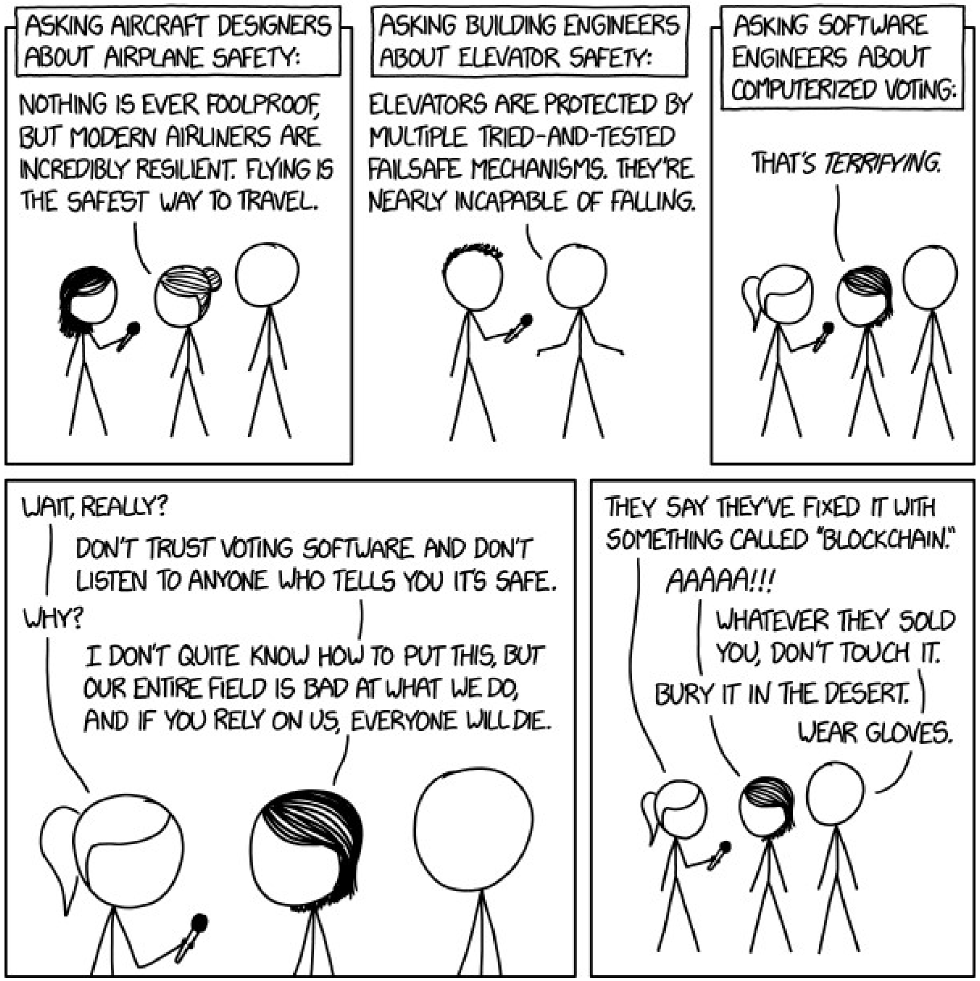
Chris Culnane
@chrisculnane

Replying to @chrisculnane

And what about that independent audit of WAEC's use of iVote, which on the topic of Incapsula said:

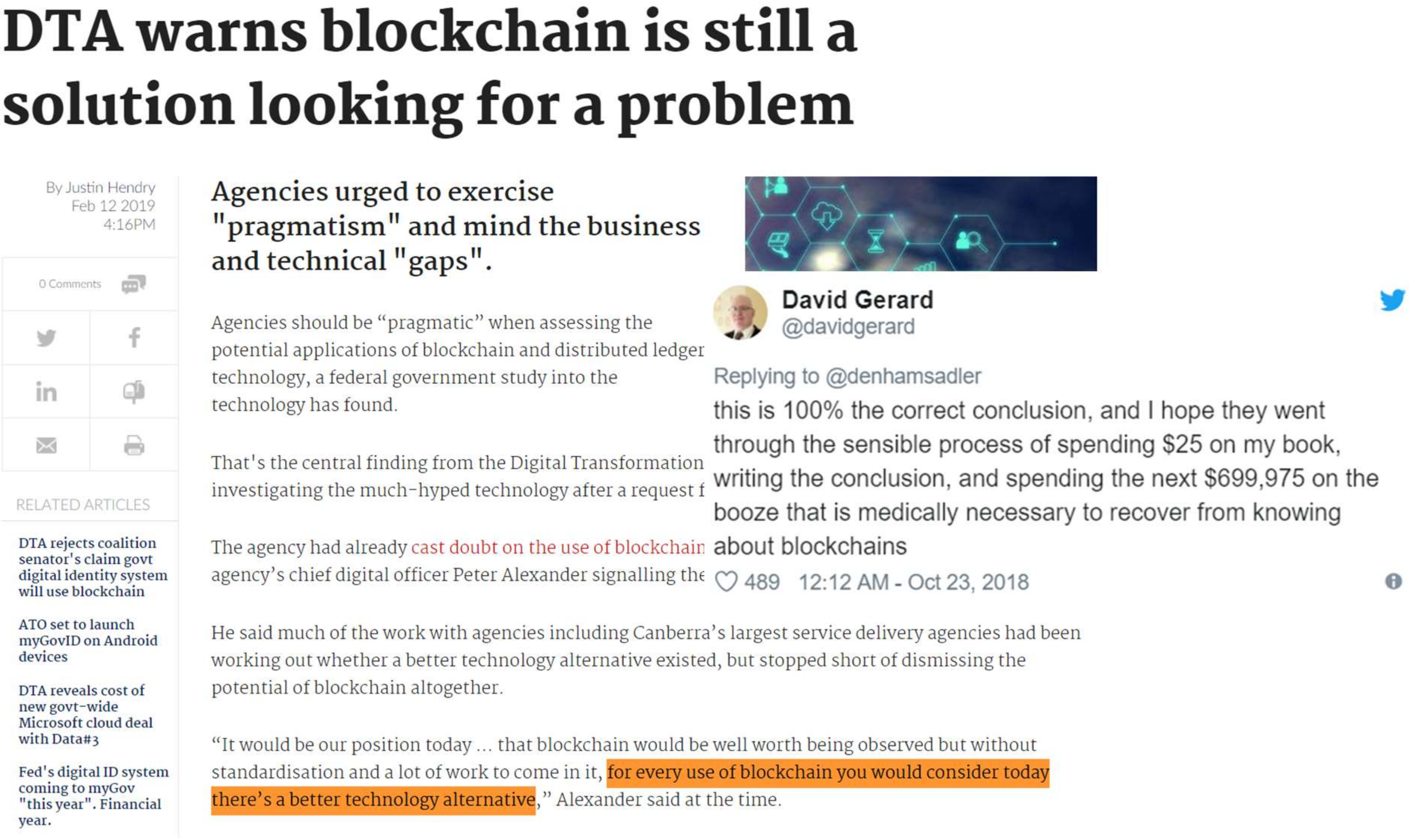
"It is my view that the chance of gaining access to the Incapsula systems is very small given their industry standing, reputation and security profile" elections.wa.gov.au/sites/default/…

♡ 1 1:53 PM - Aug 28, 2019


ASKING AIRCRAFT DESIGNERS ABOUT AIRPLANE SAFETY:
NOTHING IS EVER FOOLPROOF, BUT MODERN AIRLINERS ARE INCREDIBLY RESILIENT. FLYING IS THE SAFEST WAY TO TRAVEL.
ASKING BUILDING ENGINEERS ABOUT ELEVATOR SAFETY:
ELEVATORS ARE PROTECTED BY MULTIPLE TRIED-AND-TESTED FAILSAFE MECHANISMS. THEY'RE NEARLY INCAPABLE OF FALLING.
ASKING SOFTWARE ENGINEERS ABOUT COMPUTERIZED VOTING:
THAT'S *TERRIFYING.*
WAIT, REALLY?
DON'T TRUST VOTING SOFTWARE AND DON'T LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.
WHY?
I DON'T QUITE KNOW HOW TO PUT THIS, BUT OUR ENTIRE FIELD IS BAD AT WHAT WE DO, AND IF YOU RELY ON US, EVERYONE WILL DIE.
THEY SAY THEY'VE FIXED IT WITH SOMETHING CALLED "BLOCKCHAIN."
AAAAA!!!
WHATEVER THEY SOLD YOU, DON'T TOUCH IT.
BURY IT IN THE DESERT.
WEAR GLOVES.

"There are lots of very smart people doing fascinating work on cryptographic voting protocols. We should be funding and encouraging them, and doing all our elections with paper ballots until everyone currently working in that field has retired."

https://xkcd.com/2030/



DTA warns blockchain is still a solution looking for a problem

By Justin Hendry
Feb 12 2019
4:16PM

0 Comments

RELATED ARTICLES

- DTA rejects coalition senator's claim govt digital identity system will use blockchain
- ATO set to launch myGovID on Android devices
- DTA reveals cost of new govt-wide Microsoft cloud deal with Data#3
- Fed's digital ID system coming to myGov "this year". Financial year.

Agencies urged to exercise "pragmatism" and mind the business and technical "gaps".

Agencies should be "pragmatic" when assessing the potential applications of blockchain and distributed ledger technology, a federal government study into the technology has found.

That's the central finding from the Digital Transformation investigating the much-hyped technology after a request f

The agency had already cast doubt on the use of blockchain agency's chief digital officer Peter Alexander signalling the

He said much of the work with agencies including Canberra's largest service delivery agencies had been working out whether a better technology alternative existed, but stopped short of dismissing the potential of blockchain altogether.

"It would be our position today … that blockchain would be well worth being observed but without standardisation and a lot of work to come in it, for every use of blockchain you would consider today there's a better technology alternative," Alexander said at the time.

David Gerard
@davidgerard

Replying to @denhamsadler

this is 100% the correct conclusion, and I hope they went through the sensible process of spending $25 on my book, writing the conclusion, and spending the next $699,975 on the booze that is medically necessary to recover from knowing about blockchains

♡ 489 12:12 AM - Oct 23, 2018