

Helios

web-based open-audit voting

Ben Adida
Harvard University

IACR Voting System Session
19 August 2008

The Promise



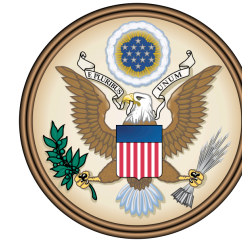
Presidential Elections 2016 Tracking Receipt

Ben Adida

65cMUev0im7KNvcHgJs/3Z2o1o0=

Machine Signature

Ys23Ag/5IOWqZCw9QGaVDdHwH00=



Presidential Elections 2016 Official Tally

Amy Aardvark

Bef1CEG0HSJrDDinnCt+gmgUQV4=

Ben Adida

65cMUev0im7KNvcHgJs/3Z2o1o0=

....

Steve Zephyr

Rfp9EIyaQARREbCWD9y9v1BZFtc=

WINNER

Britney Spears

PROOF

EbC37bnxckw02wdncxvnsdfk23508zxcvskfn234n22sdv
xb09sdfdsf0235nxvb8235324nasdfasdvxczv7234523ad
sfdvzxcv87252-5rasdfsadsvsdn2523523;42342323

“And there are cryptographic techniques that can be used to achieve software independence so that even if there's a bug in the software, you'll detect if there's a problem. **But** those are not ready for prime time in my opinion.”

Avi Rubin, 7/9/2008

“**But** with cryptography, you’re just moving the black box. **Few people** really understand it or trust it.”

Debra Bowen, 7/30/2008

(paraphrased)

Opportunity

Simplify

Low-Coercion Elections

Web-based

Core Concepts

- Benaloh Challenge.
cast or audit, authenticate only upon cast
- Homomorphic Tallying.
no write-ins, proofs of correct plaintext
- Integrity first, Privacy second.
online, tough to enforce privacy

Bag of Tricks

Single-Page Web App

```
<a href="javascript:doStuff();" >  
    next page  
</a>
```


LiveConnect

```
var p = new java.math.BigInteger("13",10);
```

```
var p = lc_applet.newBigInteger("13",10);
```

```
var GEN = new java.security.SecureRandom();
```

```
var GEN = lc_applet.newSecureRandom();
```

Data URIs

```
window.open("data:text/plain," + content);
```

```
w = window.open("");  
w.document.open("text/plain");  
w.document.write(content);  
w.document.close();
```

window.postMessage ()

```
w = window.open(HELIOS_API_URL);  
w.postMessage("election 123", helios_host);
```

```
window.addEventListener("message", ...);  
window.opener.postMessage(election_data);
```

Helios System Details

- Python & JavaScript logic & crypto
- Free/Open-Source stack
- Deployed on Google App Engine
scalable, existing defenses
- (Soon) Deployable on Apache/Python/PostgreSQL.
- Easily Customizable
authentication, look-and-feel, translations

Demo

<http://tinyurl.com/helios-crypto2008>

<http://www.heliosvoting.org/>