Helios
web-based open-audit voting

Ben Adida
Harvard University

Usenix Security – San Jose, CA
1 August 2008
VVPAT

verified-voting

crypto

homomorphic

paper-trail

mixnet
The Promise

Presidential Elections 2016
Tracking Receipt

Ben Adida
65cMUev0im7KNvcHgJs/3Z2o1o0=

Machine Signature
Ys23Ag/5IOWqZCw9QGaVDdHwH00=

Presidential Elections 2016
Official Tally

Amy Aardvark
Ben Adida
....
Steve Zephyr

WINNER
Britney Spears

PROOF
Ebc37bnxckw02wdncxvnsdfk23508zxcvsdkfn234n22sdv
xb09sdfdsf0235nxvb8235324nasdfsdcxvzv7234523sad
sfdvzxcv87252-5rasdfsadsdsn2523523;42342323

Bef1CEG0HSJrDDinnCt+gmguQV4=
65cMUev0im7KNvcHgJs/3Z2o1o0=
Rfp9EiyaQARREbCWD9y9v1BZFc=
“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)
OK. So Let’s Go.

Let’s make an open-audit voting system publicly available.
Simplify

Low-Coercion Elections

Web-based
Bag o’ Tricks
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);
Demo

http://tinyurl.com/heliosusenix
Questions?

ben@eecs.harvard.edu

http://www.heliosvoting.org/