Helios and the Edmonton Jellybean Pilot:
A Tale of Two Internet Voting Systems

Victor S. Andrei
vandrei@gmu.edu

Srinidhi Sreepad
ssreepad@gmu.edu
Agenda

- What defines a “good” voting system?

- Analysis of Internet voting systems
  - Helios (Adida, USENIX Security ’08)
  - Edmonton “jellybean” pilot in 2012

- How can we make existing systems “good”?
  - “Remote voting centers” (Sandler & Wallach, USENIX EVT ’08)
  - Use of public key cryptography
  - Paper backup for improved audit capability
What defines a “good” voting system?

| Voter eligibility and authentication | Only eligible voters may vote in an election.  
|                                      | Each eligible voter may vote only once in an election.  
|                                      | Eligible voters may only vote on behalf of themselves. |
| Ballot secrecy                       | Only individual voters should know the contents of their ballots.  
|                                      | To resist election buying, chain voting, and similar attacks, individual voters should not be able to prove the contents of their ballots to third parties. |
| Ballot verifiability                | Individual voters should be able to verify the accuracy of their ballots when they cast their ballots. |
| Ballot integrity                   | Each ballot should match the intent of the voter who cast the ballot. |
What defines a “good” voting system?

<table>
<thead>
<tr>
<th>Audit capability</th>
<th>The system should provide tools for auditing the results of an election as well as operations of the voting system’s software, hardware, and network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The system should be available during an election.</td>
</tr>
<tr>
<td>Usability</td>
<td>The system should be straightforward to use.</td>
</tr>
<tr>
<td>Enfranchisement</td>
<td>All eligible voters should have the opportunity to vote in an election.</td>
</tr>
</tbody>
</table>

Note that there may be other qualities of a “good” voting system!
Helios

- Presented in paper by Adida at USENIX Security ‘08
  - Encrypted ballot
  - Ballot verification tools
  - Smart ballot tracker

Helios is completely open source and licensed under the GPL!
ECE 646 Best Project

What is the best analytical project?

Question #1 of 1 — select at least 1 answer, up to 1 answer

- AN-1
- AN-2
- AN-3
- AN-4

Proceed
Internet Voting

ECE 646 Best Project

Your ballot was successfully encrypted

Please keep a record of your smart ballot tracker [print] [email]:

xIIV3oJ2VsjwNnGCoQKeIFk5yg43J0Ildx/3Iu1eDg8

To protect your privacy:

- Helios has not yet asked for your identity.
- Once you click “Proceed”, Helios will remember only your encrypted vote.
- Thus, only you know your vote.

Proceed to Cast

Audit [optional]

If you choose, you can audit your ballot and reveal how your choices were encrypted.

You will then be guided to re-encrypt your choices for final casting.

Verify Encryption

Election Fingerprint: Z6yxT1JUWYXyjM5zV8z6T20pwNXTNt06+wC7y/nkB

12/11/2012
ECE 646 Best Project

Your audited ballot

**IMPORTANT**: this ballot, now that it has been audited, **will not be tallied**.
To cast a ballot, you must click the ‘Back to voting’ button below, re-encrypt it, and choose “cast” instead of “audit”.

Why? Helios prevents you from auditing and casting the same ballot to provide you with some protection against coercion.

Now what? **Select your ballot audit info**, copy it to your clipboard, then use the **ballot verifier** to verify it.
Once you’re satisfied, click the “back to voting” button to re-encrypt and cast your ballot.

Before going back to voting, you can post this audited ballot to the Helios tracking center so that others might double-check the verification of this ballot.

Even if you post your audited ballot, you must go back to voting and choose “cast” if you want your vote to count.

post audited ballot to tracking center  back to voting
This single-ballot verifier lets you enter an audited ballot and verify that it was prepared correctly.

Enter the Election URL:  "https://vote.helosvoting.org/booth/single-
Your Ballot:

```
"", "$521290756007-001640677771-0016406742339314-0016406752654140-254548045910-253130305262-6", "$72412407656912211247426056819388569-222914811302117359979125266368252542-22"}], "election_hash": "Z6yxJYUYWYjMB3V8e6T20pg607b96+CC4y/nkBA", "election_
```

Verify

loading election...
election fingerprint is ZZyxJYUYWYjMB3V8e6T20pg607b96+CC4y/nkBA
smart ballot tracker is xniV3dJ2VajwNnGCcQeIF5yg430Idv/3luiuDg8
election fingerprint matches ballot
Ballot Contents:
Question #1 - What is the best analytical project? : AN-1
Encryption Verified
Proofs ok.

SUCCESSFUL VERIFICATION, DONE!
ECE 646 Best Project — Submit your Vote

We have received, but not yet recorded, your encrypted ballot.
Your smart ballot tracker is:

D8PfXqE/VxM7KUX/l+hATyga/dkBk0NDgcsbLGv1Ug

You are logged in as Victor Andrei, but this election requires election-specific credentials.
Please provide the voter ID and password you received by email.

Voter ID: 
Password: **********

Check credentials

logged in as Victor Andrei [logout]
About Helios | Help

https://vote.heliosvoting.org/helios/elections/3fd0f0a-3fd6-11e2-a0d3-l231...
ECE 646 Best Project — Submit your Vote

We have received, but not yet recorded, your encrypted ballot.
Your smart ballot tracker is:

D8PFXqE/VxM7XKUX/1+hATyga/dkBk0NDgcsbLGv1Ug

I am Victor Andrei, cast this ballot

You can cast as many ballots as you want.
Only the last one counts.

cancel

If you cancel now, your ballot will NOT be recorded.
You can start the voting process over again, of course.

https://vote.heliosvoting.org/helios/elections/3fd86f0a-3ffd-11e2-a0d0-1231...
ECE 646 Best Project — Vote Successfully Cast!

Congratulations, your vote has been **successfully cast**!

Your smart ballot tracker is:

```
D8fXqE/VxM7KUX/1+hATyga/dkBk0NDgsbLGv1Ug
```

[ return to election info ]
Edmonton “jellybean” pilot

- Test run of proprietary Internet voting system in 2012
  - “Jellybean” election
  - Verification process
    - Remote submission of identification documents
    - Election officials provided 16 character alphanumeric PIN
    - User-selected password
  - Ballot verification screen
  - Voting receipt

Panel of voters, city officials, selected experts: SUCCESS!
7. Enter the Password that you created during registration.

Edmonton Voting System

Please insert your PIN and Password

PIN: [sensitive information]
Password: [sensitive information]

Login
Internet Voting

Please select one of the options below:
November 2, 2012

Choose one (1) only
Favorite Jellybean Colour

Black
Green
Red
Yellow

Reset
Next
Your vote has been placed in the electronic ballot box. Please retain a copy of this receipt to confirm that your vote has been counted. Confirmation information should be available in the afternoon of November 2, 2012.

Receipt for the Voter

Election Name: Edmonton Elections 2012

Receipt: p6TNSXB4yl

Please take a few minutes to complete the short survey. It will help the City of Edmonton plan for future elections.
## Results - 2012 Jellybean Internet Voting Election

<table>
<thead>
<tr>
<th>Favorite Jelly Bean Colour</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black</td>
<td>123</td>
</tr>
<tr>
<td>Green</td>
<td>111</td>
</tr>
<tr>
<td>Red</td>
<td>202</td>
</tr>
<tr>
<td>Yellow</td>
<td>61</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>497</strong></td>
</tr>
</tbody>
</table>
Edmonton “jellybean” pilot

Barbara Simons  •  UC Berkeley

Asking citizens to judge Internet voting on the basis of whether or not they like it is similar to asking citizens to judge an untested medicine on the basis of whether or not it tastes good. Edmonton refused to allow outside computer security experts to test the system. I know, because I was part of a group that requested that the system be open for meaningful testing. In a real election, someone wishing to rig an Internet-based election will not ask permission. This so-called test was a travesty. The reality is that Internet voting is fundamentally insecure and impossible to recount. If there is a contested election in which Internet voting occurs, there will be no way to verify the correct winner.

Reply · 4 · Like · Follow Post · November 29 at 3:19pm

(taken from The Edmonton Journal,

Very little documentation. External security analysis was refused!

12/11/2012
## What we found

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Helios</th>
<th>Edmonton</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Voter eligibility and authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Only eligible voters may vote in an election.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>- Each eligible voter may vote only once in an election.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>- Eligible voters may only vote on behalf of themselves.</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Ballot secrecy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Only individual voters should know the contents of their ballots.</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>- To resist election buying, chain voting, and similar attacks, individual voters should not be able to prove the contents of their ballots to third parties.</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
## What we found

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Helios</th>
<th>Edmonton</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ballot verifiability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individual voters should be able to verify the accuracy of their ballots when they cast their ballots.</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Ballot integrity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Each ballot should match the intent of the voter who cast the ballot.</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Audit capability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The system should provide tools for auditing the results of an election as well as operations of the voting system’s software, hardware, and network.</td>
<td>✔️</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
What we found

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Helios</th>
<th>Edmonton</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ The system should be available during an election.</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Usability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ The system should be straightforward to use.</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Enfranchisement</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ All eligible voters should have the opportunity to vote in an election.</td>
<td>Election dependent</td>
<td>Election dependent</td>
</tr>
</tbody>
</table>

Voting from your laptop or smartphone will NEVER happen!
What we found

- **Key limitations of Internet voting**
  - Uncontrolled environment, but voting should be a controlled process
    - BYOD (voter computing device)
    - Underlying network, hardware, software
  - Ballot secrecy is impossible to guarantee

- **Open, not proprietary Internet voting systems**
  - Audit capabilities
  - Transparency requirements in voting process
  - Opportunities for comprehensive third-party security analysis
How can we make existing systems “good”?

- “Remote voting centers”
  - Proposed by Sandler and Wallach at USENIX EVT ’08
  - Networked replacement for postal voting

(taken directly from Sandler & Wallach, “The case for networked remote voting precincts,” USENIX EVT ’08)
How can we make existing systems “good”?

“Remote voting centers”
- Controlled voting environment at embassy, military base, ship
- Provisional electronic ballot
- Multiple one-way methods of transmitting encrypted, signed ballots
  - Internet link
  - Offline: CD-ROM
- Need for standardization of ballot designs between jurisdictions

Problem: one voter could cast one vote per remote voting center.
How can we make existing systems “good”?

“Remote voting centers”
  - Sandler & Wallach build on VoteBox technology from Rice, but note that Helios could be potentially used in a national election
    * Existing paperless DRE systems could also be converted

Problem: paperless DREs have been broken.
How can we make existing systems “good”? 

- Improvements to networked “paperless DREs”
  - Problems with paperless DREs described by Feldman, Halderman, and Felten at USENIX EVT ’07

Computer scientists have been skeptical of voting systems of this type, Direct Recording Electronic (DRE), which are essentially general-purpose computers running specialized election software. Experience with computer systems of all kinds shows that it is exceedingly difficult to ensure the reliability and security of complex software or to detect and diagnose problems when they do occur. Yet DREs rely fundamentally on the correct and secure operation of complex software programs. Simply put, many computer scientists doubt that paperless DREs can be made reliable and secure, and they expect that any failures of such systems would likely go undetected.


- Voter-verifiable paper audit trail system (VVPAT)

Solution: paper backup, security controls, independent review.
Questions