The **Web** Browser as a **Platform** for **Secure** Applications.

Ben Adida
Harvard

CRCS Luncheon
14 May 2008
Web Pages are Programs
Web Pages are Programs

<head>
  <title>Random Blog</title>
  <script src="http://www.google-analytics.com/urchin.js" type="text/javascript">
  </script>
</head>
Introspection
Introspection

document.getElementById('article_content').innerHTML;

Network Requests

var req = new XMLHttpRequest();

req.onreadystatechange = function() {
  if (req.readyState == 4) {
    // do something with req.responseText
  }
};

req.open("GET", "/more-data", true);
req.send(""
Introspection

```javascript
var req = new XMLHttpRequest();
req.onreadystatechange = function() {
    if (req.readyState == 4) {
        // do something with req.responseText
    }
};
req.open("GET", "/more-data", true);
req.send("");
```

Network Requests

```javascript
var req = new XMLHttpRequest();
req.onreadystatechange = function() {
    if (req.readyState == 4) {
        // do something with req.responseText
    }
};
req.open("GET", "/more-data", true);
req.send("");
```

Modifying the Page

```javascript
document.getElementById('menu').style.display = 'none';
var i = document.createElement('img');
i.src = 'http://otherdomain.com/photo2.jpg';
document.body.appendChild(i);
```
BigBank.com

MyFriendBook.com

GET /friends

User

BigBank.com Cookie
sessionid=8d8c93200
BigBank.com Cookie
sessionid=8d8c93200

GET
/friends

Bank balance
stealing code

User
BigBank.com

User

MyFriendBook.com

GET /balance

Bank balance stealing code

BigBank.com Cookie
sessionid=8d8c93200
BigBank.com

MyFriendBook.com

GET /friends

Bank balance stealing code

GET /balance

User

BigBank.com Cookie sessionid=8d8c93200

$42
BigBank.com

User

MyFriendBook.com

Cookie

sessionid=8d8c93200

GET
/balance

$42

GET
/friends

Bank balance stealing code

$42
Intranet

User
Intranet

MyFriendBook.com

GET /friends

Port scan code

User
Intranet

GET /employees

MyFriendBook.com

GET /friends

Port scan code
Intranet

GET /employees

"Alice, Bob,..."

GET /friends

Port scan code

MyFriendBook.com
Intranet

User

MyFriendBook.com

GET /friends

Port scan code

"Alice, Bob,..."

GET /employees

"Alice, Bob,..."
Intranet

MyFriendBook.com

GET /friends
Port scan code

"Alice, Bob,..."

GET /employees

"Alice, Bob,..."

User
Cross-Domain Images

flickr.com

MyBlog.com

User
Cross-Domain Images

flickr.com

GET /post?id=3
Blog Post w/ Inline image

MyBlog.com

User
Cross-Domain Images

flickr.com

GET /photo

MyBlog.com

GET /post?id=3

Blog Post w/ Inline image

User
Cross-Domain Images

flickr.com

GET /photo

MyBlog.com

GET /post?id=3

Blog Post w/ Inline image

User
Cross-Domain Scripts
Cross-Domain Scripts

<head>
<title>Random Blog</title>

<script src="http://www.google-analytics.com/urchin.js" type="text/javascript">
</script>

</head>
Cross-Domain Scripts

```html
<head>
  <title>Random Blog</title>
  <script src="http://www.google-analytics.com/urchin.js" type="text/javascript">
  </script>
</head>

var new_script = document.createElement('script');
new_script.src = 'http://otherdomain.com/';
document.head.appendChild(new_script);
```
Cross-Domain Scripts

```html
<head>
  <title>Random Blog</title>

  <script src="http://www.google-analytics.com/urchin.js" type="text/javascript">
  </script>
</head>

var new_script = document.createElement('script');
new_script.src = 'http://otherdomain.com/';
document.head.appendChild(new_script);
```
State of Cross-Domain
State of Cross-Domain

• Cross-Domain outgoing messages can always be sent (using, IMG, SCRIPT, FORM, or IFRAME.)
State of Cross-Domain

• Cross-Domain outgoing messages can always be sent (using, IMG, SCRIPT, FORM, or IFRAME.)

• Cross-Domain incoming data can be integrated in limited ways:
  ➡ images rendered, but opaquely
  ➡ scripts executed, but opaquely
State of Cross-Domain
State of Cross-Domain

• XHR2 with Access Control:
  allowing third-party HTTP requests.
State of Cross-Domain

- XHR2 with Access Control: allowing third-party HTTP requests.
- Server must opt in to 3rd-party GET: browser grants access on opt-in.
State of Cross-Domain

- XHR2 with Access Control: allowing third-party HTTP requests.
- Server must opt in to 3rd-party GET: browser grants access on opt-in.
- Server must opt in to 3rd-party POST: server must opt-in before POST is sent.
State of Cross-Domain

- **XHR2 with Access Control:** allowing third-party HTTP requests.
- **Server must opt in to 3rd-party GET:** browser grants access on opt-in.
- **Server must opt in to 3rd-party POST:** server must opt-in before POST is sent.

**Question:** should browsers send cookies for third-party requests?
Classic Security Model
Classic Security Model

Master Site
Classic Security Model

Master Site

Eve

Evil Browser
Classic Security Model

Master Site

Eve

Evil Browser
New Security Model
New Security Model

Master Site
New Security Model

Master Site

Alice
New Security Model

Evil Third Party

Master Site

Alice
New Security Model

Evil Third Party  Master Site

Alice

Standard Browser
Building a Secure Browser Platform is Hard.

What can we do now?
Security in the App Layer
Security in the App Layer

HTTP
Security in the App Layer

- HTML & JavaScript
- HTTP
Security in the App Layer

- Application Code
- HTML & JavaScript
- HTTP
Security in the App Layer

- Application Code
- HTML & JavaScript
- HTTP
Security in the App Layer

- Can we build better security in the application layer?
Security in the App Layer

- Can we build better security in the application layer?
- Maybe by hijacking certain features for security purposes? (Active Cookies, Subspace, ...)

Application Code

HTML & JavaScript

HTTP
Security in the App Layer

- Can we build better security in the application layer?
- Maybe by hijacking certain features for security purposes? (Active Cookies, Subspace, ...)

Goal: provide new, unexpected security features
BeamAuth
Two-Factor Web Auth
with a Bookmark

[CCS 2007]
Sad State of Web Auth
Sad State of Web Auth
Sad State of Web Auth

Check your address book to see who uses LinkedIn

Yahoo!  America Online  Gmail  Hotmail

Check webmail contacts

Don't use webmail?
Sad State of Web Auth

Search your webmail address book for friends.

Your Email: [input field] @ [input field]

Email Password: [input field]

Find Your Friends

⚠️ We won't store your login info or contact anyone without your permission.

Use Outlook, Apple Mail, Thunderbird or others?
We can also import your address book.
SSO makes things worse
SSO makes things worse
SSO makes things worse
SSO makes things worse
SSO makes things worse
Update the Browser

- **Dynamic Security Skins** [DT2005]
  secure password-based key exchange
  new browser chrome to auth web site.

- **PwdHash** [RJMBM2005]
  domain-specific password pre-processing.

- **MS CardSpace**
  change the entire auth infrastructure
  built into the operating system.
The General Idea
The General Idea

Setup Phase

Alice

Login Phase

OpenID Server
The General Idea

Setup Phase

Alice

proof of identity

OpenID Server

Login Phase
The General Idea

Setup Phase

Alice

proof of identity

OpenID Server

token

Login Phase
The General Idea

Setup Phase

Alice

proof of identity

token

OpenID Server

Login Phase

Click Your BeamAuth Login Button
The General Idea

Setup Phase

Alice

proof of identity

token

OpenID Server

Login Phase

Click Your BeamAuth Login Button
The General Idea

- [Image]
  - Setup Phase
  - Alice
  - OpenID Server
  - proof of identity
  - token
  - Login Phase
    - Click Your BeamAuth Login Button
    - Username benadida
    - Password
    - log in
The General Idea

Setup Phase

proof of identity

Alice

token

OpenID Server

Login Phase

Click Your BeamAuth Login Button

Username benadida
Password **********
log in
The General Idea

Setup Phase

Alice

proof of identity

token

Welcome, Ben Adida.

Login Phase

Click Your BeamAuth Login Button

Username benadida
Password **********
log in
Let’s Build this Button!
Let’s Build this Button!

- **Browser add-on**
  not an easy solution for most users
  complexity of add-on across browsers
  significant trust delegated to the login site
Let’s Build this Button!

- **Browser add-on**
  not an easy solution for most users
  complexity of add-on across browsers
  significant trust delegated to the login site

- **Bookmark**
  Delicious, etc. use bookmarks as buttons
  can we do the same for security?

BookMark Auth = BM Auth = **BeamAuth**
JavaScript Bookmarks
javascript:document.location='http://del.icio.us/add?u=' + encodeURIComponent(document.location);
JavaScript Bookmarks

```javascript
javascript:document.location='http://del.icio.us/add?u=' + encodeURIComponent(document.location);

javascript:beamauth_token('x737csd23');
```
JavaScript Bookmarks

```
javascript:document.location='http://del.icio.us/add?u=' + encodeURIComponent(document.location);

javascript:beamauth_token('x737csd23');
```
JavaScript Bookmarks

document.location='http://del.icio.us/add?u=' + encodeURIComponent(document.location);

beamauth_token('x737csd23');

if (document.location.hostname == 'myopenid.com'){
  beamauth_token('x737csd23');
}
javascript:document.location='http://del.icio.us/add?u=' + encodeURIComponent(document.location);

javascript:beamauth_token('x737csd23');

javascript:
if (document.location.hostname == 'myopenid.com'){
    beamauth_token('x737csd23');
}
JavaScript Bookmarks

```javascript
document.location='http://del.icio.us/add?u=' + encodeURIComponent(document.location);
beamauth_token('x737csd23');
if (document.location.hostname == 'myopenid.com'){
  beamauth_token('x737csd23');
}
```

Cannot trust the JavaScript Computing Base
The URL Fragment Identifier

http://site.com/page#paragraph
The URL Fragment Identifier

http://site.com/page#paragraph

- used to designate a portion of a page
  browser scrolls to the appropriate location.
The URL Fragment Identifier

http://site.com/page#paragraph

- used to designate a portion of a page
  browser scrolls to the appropriate location.

- _never sent_ over the network but accessible from JavaScript
The URL Fragment Identifier

http://site.com/page#paragraph

- used to designate a portion of a page
  browser scrolls to the appropriate location.

- *never sent* over the network but accessible from JavaScript

- navigation between fragments does not cause a page reload.
Fragment in a Bookmark

http://login.com/login#[benadidal8x34202]
Fragment in a Bookmark

http://login.com/login#[benadidal8x34202]

```javascript
var hash = document.location.hash;

if (hash != '') {
    // parse the hash, get username and token
    process_beamauth_hash(hash);

    // clear the hash from the URL
    document.location.replace('~/login');
}
```
The BeamAuth Ritual
The BeamAuth Ritual

BeamAuth Authentication Demo

part of BeamAuth

you are not logged in.

Click your BeamAuth bookmark to log in.

register | forgot your password? | lost your BeamAuth Bookmark

Email: ben@adida.net
Password: ****
Password (confirm): ****
The BeamAuth Ritual

Subject: BeamAuth Setup
From: BeamAuth Administrator <beamauth@adida.net>
Date: 7:23 PM
To: ben@adida.net
Tags: Personal

You have successfully registered at BeamAuth Bookmark Authentication.
Follow this link to obtain your BeamAuth bookmark.

http://ben.adida.net/projects/beamauth/demo/confirm?email=ben

-BeamAuth Admin
The BeamAuth Ritual

BeamAuth Bookmark Setup

part of BeamAuth

You've been confirmed. You should now drag this special login bookmark to your

BeamAuth

And now, go login.
The BeamAuth Ritual

BeamAuth Bookmark Setup

You've been confirmed. You should now drag this special login bookmark to your bookmarks.

And now, go login.
The BeamAuth Ritual

BeamAuth Authentication Demo
part of BeamAuth

you are not logged in.

Click your BeamAuth bookmark to log in.

register | forgot your password? | lost your BeamAuth Bookmark
The BeamAuth Ritual

BeamAuth Authentication Demo
part of BeamAuth

you are not logged in.

Click your BeamAuth bookmark to log in.

Email: ben@adida.net
Password: login!
The BeamAuth Ritual

BeamAuth Authentication Demo
part of BeamAuth

you are logged in as ben@adida.net

log out.
Attacks

- Trick User into Not Clicking Bookmark
  password compromised, token safe.

- Lock User into Site
  password compromised, token safe.

- Maliciously Replace Bookmark
  password compromised, token safe.

- Pharming
  all compromised.

- “Drag-and-Drop” Attack
  all compromised on Firefox.
Comparison to Long-Lasting Cookies

- **Second-channel setup** – though long-lasting cookies could do the same thing there.

- **Synchronization** across browsers using existing bookmark-sync tools.

- Better behavior for **non-SSL** sites
**BeamAuth: Summary**

- Bookmark as second authentication factor
- Token delivered via a separate channel (email)
- Use the fragment identifier to store token
- Tweaked Login Ritual: whisk users to safety
Anything else with that fragment?
SessionLock
Securing HTTP Sessions from Eavesdroppers
wi-fi typically unencrypted, easy to sniff.
Web Browser

Web Server

SetCookie: uid=12345; tok=87654

/login?username&password
SetCookie: uid=12345; tok=87654

Cookie: uid=12345; tok=87654

Web Browser

Web Server

/login?username&password

/inbox

Cookie: uid=12345; tok=87654

contents of inbox
The diagram illustrates a web application with a login route `/login?username&password` that sets a cookie `SetCookie: uid=12345; tok=87654`. A request to `/inbox` includes a cookie `Cookie: uid=12345; tok=87654`. An attacker, Eve, intercepts the cookie and can access the contents of the inbox.
Web Browser

Web Server

SetCookie: uid=12345;tok=87654

Cookie: uid=12345;tok=87654

/inbox

contents of inbox

Cookie: uid=12345;tok=87654

/send?to=billg

Eve

Cookie: uid=12345;tok=87654

uid=12345;tok=87654
SSL?

- Content Distribution Networks
- All-or-Nothing Content
- All-or-Nothing Download
- Caching
SSL?

- Content Distribution Networks
- All-or-Nothing Content
- All-or-Nothing Download
- Caching

Even with server-side horsepower, SSL is significantly more sluggish.
Encryption is not the Issue

- add a few lines to a wiki
- check a few notifications on gmail
- send a few pages to my bookmarks aggregator
Encryption is not the Issue

- add a few lines to a wiki
- check a few notifications on gmail
- send a few pages to my bookmarks aggregator

Risk: complete impersonation!
Encryption is not the Issue

- add a few lines to a wiki
- check a few notifications on gmail
- send a few pages to my bookmarks aggregator

Risk: complete impersonation!

Shoulder-surfing my email is not the end of the world. Impersonating me to my webmail is much worse.
Current Login Approach

Web Server

Web Browser
Current Login Approach

Web Browser

Web Server

Set-Cookie: uid=12345; tok=87654

/inbox

contents of inbox

/login?username&password
The **SessionLock** Idea
The **SessionLock** Idea

- Use the SSL login to send a **SECRET** to the web browser.
The **SessionLock** Idea

- Use the SSL login to send a **SECRET** to the web browser.

- “Pass” **SECRET** to the non-SSL side.
The **SessionLock** Idea

- Use the SSL login to send a **SECRET** to the web browser.
- "Pass" **SECRET** to the non-SSL side.
- Keep **SECRET** in scope, use it to sign every HTTP request.
The **SessionLock** Idea

- Use the SSL login to send a `SECRET` to the web browser.
- “Pass” `SECRET` to the non-SSL side.
- Keep `SECRET` in scope, use it to sign every HTTP request.
- Never send `SECRET` in plaintext.
Passing Secret via Fragment

http://webmail/#SECRET
Passing Secret via Fragment

http://webmail/#SECRET

```javascript
var hash = document.location.hash;

if (hash != '') {
    // parse the hash, get username and token
    store_secret(hash);

    // clear the hash from the URL
    document.location.replace('http://webmail/');
}
```
Signing with HMAC
Signing with HMAC

- Assume a single-page web application (for now).
Signing with HMAC

- Assume a single-page web application (for now).
- Intercept all XHR JavaScript requests
Signing with HMAC

- Assume a single-page web application (for now).
- Intercept all XHR JavaScript requests
- append timestamp, HMAC the request line, append HMAC result.

\[
\text{sig} = \text{HMAC}_{\text{secret}}(\text{"/message?id=3&ts=20080514.."})
\]

/message?id=3&ts=20080514..&s=sig
Signing with HMAC

- Assume a single-page web application (for now).
- Intercept all XHR JavaScript requests
- Append timestamp, HMAC the request line, append HMAC result.

\[ \text{sig} = \text{HMAC}_{\text{secret}}("/message?id=3&ts=20080514..") \]
\[/message?id=3&ts=20080514..&s=sig\]

- 50ms on a 3-year-old laptop for each request (much faster on recent laptop with FF3.)
Web Browser

Web Server

/login?username&password
Web Browser

Web Server

Cookie: bd5c

/login?username&password

302 /mail#[ac8f]
Web Server

Web Browser

Cookie: bd5c

/login?username&password

302 /mail#[ac8f]

/launch
Web Server

Web Browser

Cookie: bd5c

JS+HTML interface

302 /mail#[ac8f]

/layout

/login?username&password
Web Server

Web Browser

Cookie: bd5c

Load #[ac8f] from fragment and store in JavaScript scope.
Load #[ac8f] from fragment and store in JavaScript scope.
Web Server

Web Browser

Cookie: bd5c

Load #[ac8f] from fragment and store in JavaScript scope.
Web Browser

Web Server

Cookie: bd5c

Load #[ac8f] from fragment and store in JavaScript scope.

1. `/login?username&password`
2. `/launch`
3. `/inbox?date&HMAC`
4. List of emails in inbox
5. JS+HTML interface
6. 302 `/mail#[ac8f]`
Recovery

Web Server

Web Browser

Cookie: bd5c

Load #[ac8f] from fragment and store in JavaScript scope.

/launch

JS+HTML interface

302 /mail#[ac8f]

/login?username&password

Load #[ac8f] from fragment and store in JavaScript scope.
Recovery

Web Server

Web Browser

/launch

302 /mail#[ac8f]

JS+HTML interface

Cookie: bd5c

Cookie: ac8f

Load #[ac8f] from fragment and store in JavaScript scope.
Recovery

Web Browser

Web Server

Cookie: bd5c

Load #[ac8f] from fragment and store in JavaScript scope.

Cookie: ac8f

302 /mail#[ac8f]

302 /login?username&password

/launch

JSL+HTML interface

/inbox?date&HMAC

List of emails in inbox
Recovery

http://webmail/

*missing secret token*
Recovery

http://webmail/

https://webmail/recover

tok = cookie('tok');
location = 'http://webmail/
  recover#' + tok;

open dynamic iframe
Recovery

http://webmail/

```
tok = get_fragment();
window.parent.
  set_tok(tok);
```

recover token
token recovered, close frame, make AJAX requests
Multi-Page Apps

- need to keep the secret around from page to page.
- can’t be done on the server side, as it would then be sent unencrypted.
- must be done as a side-channel on the client side.
Multi-Page Apps
Multi-Page Apps

Web Server

/login?username&password

302 /mail#[ac8f]

Web Browser
Multi-Page Apps

Web Server

/login?username&password

302 /mail#[ac8f]

Web Browser

Cookie: bd5c
Multi-Page Apps

Web Server

Web Browser

Cookie: bd5c
Multi-Page Apps

Web Server

Web Browser

Cookie: bd5c

/login?username&password

302 /mail#[ac8f]

/launch

#[ac8f]
Multi-Page Apps

Web Server

/login?username&password

302 /mail#[ac8f]

Cookie: bd5c

launch

launch page

Web Browser
Multi-Page Apps

Web Server

Web Browser

/launch

Cookie: bd5c

302 /mail#[ac8f]

launch page

Load #[ac8f] from fragment use to HMAC and patch links.
Multi-Page Apps

Web Server

Web Browser

Cookie: bd5c

Load #[ac8f] from fragment use to HMAC and patch links.
Multi-Page Apps

Web Server

Web Browser

Cookie: bd5c

302 /mail?#[ac8f]

/labn?username&password

launch

launch page

/inbox?date&HMAC

Load #[ac8f] from fragment
use to HMAC and patch links.
Multi-Page Apps

Web Server

/launch

Cookie: bd5c

/load

302 /mail#[ac8f]

list of emails

launch page

/inbox?date&HMAC

Load #[ac8f] from fragment use to HMAC and patch links.
Multi-Page Apps

Web Server

Web Browser

Cookie: bd5c

Load #[ac8f] from fragment used to patch links with HMAC.

Load #[ac8f] from fragment use to HMAC and patch links.
Better Page-to-Page Transfer & Recovery
Better Page-to-Page Transfer & Recovery

/*
  * Browser-Local Storage
  */

// store the token as soon as it is obtained.
globalStorage['webmail.com'].session_key = '...';

// On opening up a new browser window, get token.
var session_key = globalStorage['webmail.com']
SessionLock Summary
SessionLock Summary

- fragment identifier as a client-only channel between HTTPS and HTTP.
SessionLock Summary

- fragment identifier as a client-only channel between HTTPS and HTTP.
- AJAX single-page application is easy.
SessionLock Summary

- fragment identifier as a client-only channel between HTTPS and HTTP.
- AJAX single-page application is easy.
- Multi-page apps:
SessionLock Summary

- fragment identifier as a client-only channel between HTTPS and HTTP.
- AJAX single-page application is easy.
- Multi-page apps:
  - keep the secret around by frag id.
SessionLock Summary

- fragment identifier as a client-only channel between HTTPS and HTTP.
- AJAX single-page application is easy.
- Multi-page apps:
  - keep the secret around by frag id.
  - small JS library that patches HTML.
SessionLock Summary

- fragment identifier as a client-only channel between HTTPS and HTTP.
- AJAX single-page application is easy.
- Multi-page apps:
  - keep the secret around by frag id.
  - small JS library that patches HTML.
  - writing your app with SessionLock in mind.
SessionLock Summary
SessionLock Summary

Intuition matches threat model more closely.

What you browse is visible to an eavesdropper.
What you don’t browse is safe.

Actions with side-effects are safe.
Helios
Web-based
Open-Audit Voting

[Usenix Security 2008]
Public Ballots

Bridget: McCain

Carol: Obama
Public Ballots

Bridget: McCain

Carol: Obama

Alice
Public Ballots

Alice: Obama

Bridget: McCain

Carol: Obama

Alice
Public Ballots

Alice: Obama
Bridget: McCain
Carol: Obama

Tally
Obama: 2
McCain: 1
Encrypted Public Ballots

Alice: Rice
Bridget: Clinton
Carol: Rice

Tally
Obama....2
McCain....1
Encrypted Public Ballots

Alice: Rice
Bridget: Clinton
Carol: Rice

Tally: Obama...2
McCain...1

Alice verifies her vote
Encrypted Public Ballots

Alice: Rice
Bridget: Clinton
Carol: Rice

Tally: Obama....2
McCain....1

Alice verifies her vote
Everyone verifies the tally
Benaloh Casting Protocol
Benaloh Casting Protocol

Alice

Benaloh Casting Protocol

[Diagram of a person (Alice) pointing to a device]

Benaloh Casting Protocol

Benaloh Casting Protocol
Benaloh Casting Protocol

Alice

Encrypted Ballot

"AUDIT"

Alice

Benaloh Casting Protocol
Benaloh Casting Protocol

Alice

Encrypted Ballot

Decrypted Ballot

"AUDIT"

VERIFICATION

Benaloh Casting Protocol

Benaloh Casting Protocol

Benaloh Casting Protocol
Benaloh Casting Protocol

Alice

Decrypted Ballot

"AUDIT"

Encrypted Ballot

Decrypted Ballot

"CAST"

VERIFICATION

Benaloh Casting Protocol

AUDIT

Decrypted Ballot

CAST

Signed Encrypted Ballot

VERIFICATION

Benaloh Casting Protocol

- Alice
- Encrypted Ballot
- Signed Encrypted Ballot
- "CAST"
- "AUDIT"
- Decrypted Ballot
- VERIFICATION

Benaloh Casting Protocol

Alice

Encrypted Ballot

Decrypted Ballot

Signed Encrypted Ballot

Verified

Filling out a Ballot

Helios Voting Booth: JFK High School
Student Government 2008

back to election

President (please select 1 answer)

What is your selection for Student Government President?

- [ ] Adam
- [ ] Beatrice
- [ ] Carol

[Next]  [Done]
Encrypting a Ballot

Helios Voting Booth: JFK High School Student Government 2008

Confirmation of your Choices

President: Adam
[review]

Secretary: Elise
[review]

[seal]
Encrypting a Ballot

Helios Voting Booth: JFK High School Student Government 2008

Your sealed ballot

Your vote has now been encrypted, and the fingerprint of your encrypted vote is:

cTYZy//huzKYMxk9epa7oWvFyQ
[Your Receipt] [Your Receipt by Email]

If you choose to cast the ballot, all plaintext information will be deleted from your browser's memory. Then, you will be prompted for your email and

You can choose to audit your vote, which will show you how your options were encrypted. If you do so, you will then have to re-vote, since, in a secret ballot, you cannot obtain proof of how you voted.

[audit]
Encrypting a Ballot
Encrypting a Ballot

// Call Java from JavaScript
var a = new java.math.BigInteger(42);
var b = new java.math.BigInteger(17);
var c = new java.math.BigInteger(12);

alert(a.modPow(c, b).toString());
Encrypting a Ballot

// Call Java from JavaScript
var a = new java.math.BigInteger(42);
var b = new java.math.BigInteger(17);
var c = new java.math.BigInteger(12);

alert(a.modPow(c, b).toString());

// Call Java from JavaScript (IE & Safari)
var a = MyApplet.static_new_bigint(42);
...
Getting a Receipt

Helios Voting Booth: JFK High School Student Government 2008

Your sealed ballot

Your vote has now been encrypted, and the fingerprint of your encrypted vote is:

ctYZy//huzKymaxk9epa7oWvFyQ

[Your Receipt] [Your Receipt by Email]

If you choose to cast the ballot, all plaintext information will be deleted from your browser's memory. Then, you will be prompted for your email and

You can choose to audit your vote, which will show you how your options were encrypted. If you do so, you will then have to re-vote, since, in a secret ballot, you cannot obtain proof of how you voted.

audit
Getting a Receipt
Getting a Receipt

// open a Data URI
<a target="_new"
   href="data:text/plain,Your%20Receipt...">receipt
</a>
Getting a Receipt

// open a Data URI
<a target="_new"
    href="data:text/plain,Your%20Receipt...">receipt
</a>

// dynamic construction of a window
var receipt = window.open();
receipt.document.open("text/plain");
receipt.document.write(content);
receipt.document.close();
Confirm

Are you sure you want to navigate away from this page?

If you leave this page with an in-progress ballot, your ballot will be lost.

Press OK to continue, or Cancel to stay on the current page.
Thoughts

- Guide developers to “do the right thing.”
- Let the browser become a true platform
- Security solutions in the application layer
- ideally through design, not tricks
Thoughts

- Guide developers to “do the right thing.”
- Let the browser become a true platform
- Security solutions in the application layer
- ideally through design, not tricks

Should browsers send cookies for third-party requests? YES.
Questions?

ben_adida@harvard.edu

http://ben.adida.net/