BeamAuth
Two-Factor Web Auth
with a Bookmark

Ben Adida
Harvard University

CCS 2007 – Alexandria, VA
30 October 2007
Can we improve web security without upgrading the browser?
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
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.
Can We Do Something **Now**?
Can We Do *Something* Now?
Can We Do Something **Now?**

- HTML & JavaScript
- HTTP
Can We Do *Something Now?*

- Application Code
- HTML & JavaScript
- HTTP
Can We Do *Something* Now?

- Application Code
- HTML & JavaScript
- HTTP
Can We Do *Something* Now?

- The web is a (limited) platform
Can We Do *Something Now*?

- The web is a (limited) platform
- Can we build better security in the application layer?
Can We Do *Something* **Now?**

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

**Diagram:**

- **Application Code**
- **HTML & JavaScript**
- **HTTP**
Can We Do *Something* **Now?**

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

**Goal: preventing easy phishing**
The General Idea

Setup Phase

Login Phase
The General Idea

Setup Phase

Alice

Login Phase

OpenID Server
The General Idea

Setup Phase

Alice

proof of identity

Login Phase

OpenID Server
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

OpenID Server

token

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

Username

Password

log in
The General Idea

Setup Phase

Alice

proof of identity

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

OpenID Server

Login Phase

Click Your BeamAuth Login Button

Welcome,
Ben Adida.

Username: benadida
Password: **********

Welcome,
Ben Adida.
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 Bookmarks

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

javascript:beamauth_token('x737csd23');
JavaScript Bookmarks

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

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

```javascript
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');
}
```

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

- 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

```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): ****

register
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

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

And now, go login.
The BeamAuth Ritual

BeamAuth Bookmark Setup

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

And now, go login.
The BeamAuth Ritual

BeamAuth Authentication Demo

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
Can we do more?

- The fragment identifier might be used for more tricks.
- JavaScript bookmarks may be useful for security.
- Security in the app layer: help evolve the browser platform without anticipating all security requirements.

generalize concept of site-specific extension?
Questions?

ben@eecs.harvard.edu

http://ben.adida.net/projects/beamauth/