Contextual Identity:

Supporting multiple identities on the web

Steven Englehardt
About Me

- Princeton CS PhD Student
- I do web privacy research
- I worked on two Mozilla projects this summer
  - I’ll present the second one, which I’ve been working on for almost 6 weeks.

Github: englehardt
Research: webtab.princeton.edu
Personal: cs.princeton.edu/~ste/
What is Contextual Identity?
We have multiple identities in life.
We have multiple identities in life.

At Work
We have multiple identities in life.

At Work

With Friends
We have multiple identities in life.

At Work

With Friends

With Family
We have multiple identities in life.

At Work

With Friends

With Family

Anonymous Online
We also have multiple identities online.

- Multiple email accounts
- Multiple Facebook profiles
- Different identities on different sites
Why are things this way?
Why are things this way?

Browser

example.com

<table>
<thead>
<tr>
<th>domain</th>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why are things this way?

Browser | example.com

Request: example.com
Why are things this way?

Browser

Request: example.com

Response

Set-Cookie: abc=12345

<table>
<thead>
<tr>
<th>domain</th>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why are things this way?

Browser

Request: example.com

Response

Set-Cookie: abc=12345

<table>
<thead>
<tr>
<th>domain</th>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>abc</td>
<td>12345</td>
</tr>
</tbody>
</table>
Why are things this way?

Browser

Request: example.com

Response
Set-Cookie: abc=12345

Request: example.com
Cookie: abc=12345

<table>
<thead>
<tr>
<th>domain</th>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>abc</td>
<td>12345</td>
</tr>
</tbody>
</table>
Why are things this way?

Browser

Request: example.com

Response
Set-Cookie: abc=12345

Request: example.com
Cookie: abc=12345

Request: example.com
Cookie: abc=12345

example.com

<table>
<thead>
<tr>
<th>domain</th>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>abc</td>
<td>12345</td>
</tr>
</tbody>
</table>
Cookies

1. Sent with every request
2. Sent with any request, regardless of the cause of that request
   a. Top level site
   b. Framed site
   c. Redirect
This causes a lot of problems

**Privacy**
- Tracking
- Cookie syncing

**Security**
- Clickjacking
- CSRF
- XSS
All of your cookies are in one jar.
All of your cookies are in one jar.

You don’t control when your cookies are sent.
All of your cookies are in one jar.

You don’t control when your cookies are sent.

You can’t have multiple identities.
What can users do?
1. Use Multiple Browsers
1. Use Multiple Browsers

Or rather...
1. Use Multiple Browsers

Or rather...

Clunky Experience
2. Private Browsing Mode
2. Private Browsing Mode

- Not Persistent
- Re-authenticate (2 factor)
- Only 2 profiles
3. Add-ons that help isolate state

Priv8

Multifox
What did we do?
Give users the ability to determine which set of cookies to send
Give users the ability to determine which set of cookies to send

Home
Work
Banking
???
How?

<table>
<thead>
<tr>
<th>domain</th>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bugzilla.com</td>
<td>abc</td>
<td>12345</td>
</tr>
<tr>
<td>chase.com</td>
<td>def</td>
<td>09876</td>
</tr>
<tr>
<td>twitter.com</td>
<td>xyz</td>
<td>00000</td>
</tr>
</tbody>
</table>
How?

<table>
<thead>
<tr>
<th>domain</th>
<th>userContextId</th>
<th>name</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bugzilla.com</td>
<td>0</td>
<td>abc</td>
<td>12345</td>
</tr>
<tr>
<td>chase.com</td>
<td>0</td>
<td>def</td>
<td>09876</td>
</tr>
<tr>
<td>twitter.com</td>
<td>0</td>
<td>xyz</td>
<td>00000</td>
</tr>
</tbody>
</table>
But things aren’t so simple...

- ID checks are needed everywhere
  - e.g. cookies, cache, localStorage, ...
  - All origin checks need to be updated

- We’re not the first to need to do this
  - Firefox OS keys storage using AppId
OriginAttributes

dictionary OriginAttributesDictionary {
    unsigned long appId = 0;
    unsigned long userContextId = 0;
    boolean inBrowser = false;
    DOMString addonId = "";
};

- Origin checks done against the OriginAttributes dictionary/struct, not against individual IDs.

- Ongoing effort led by Yoshi Huang and Bobby Holley
The User Interface
Thanks for choosing Firefox! To get the most out of your browser, learn more about the latest features.
Drive away in your dream car
Desired Functionality
The Next Steps

1. Prototype behind a pref in Nightly
   - `privacy.userContext.enabled`
   - *Timeline: next few weeks*
The Next Steps

1. Prototype behind a pref in Nightly
   - privacy.userContext.enabled
   - *Timeline: next few weeks*

2. originAttributes Support
   - Many components need updates
   - userContextID *automatically supported*
   - *Timeline: next couple months*
The Next Steps

1. Prototype behind a pref in Nightly
   - `privacy.userContext.enabled`
   - *Timeline: next few weeks*

2. `originAttributes` Support
   - Many components need updates
   - `userContextID` automatically supported
   - *Timeline: next couple months*

3. Iterate on prototype
   - Add context management features
   - Incorporate user testing
   - *Timeline: depends*
I’ve had a lot of help

- **Mentor:** Tanvi Vyas
- **UX Designer:** Bram Pitoyo
- Monica Chew, Sid Stamm
  - Contextual Identity: Freedom to be All Your Selves
- Entire Content Security Team
- Yoshi Huang, Bobby Holley, and the Firefox OS team
- The University Team

*Image assets from the Noun Project:
Find out more

**Project Wiki:** wiki.mozilla.org/Security/Contextual_Identity_Project/Containers

**User Contexts/Containers Implementation:** Bug 1191418

**OriginAttributes Implementation:** Bug 1179985

**Github:** englehardt

**Research:** webtab.princeton.edu

**Personal:** cs.princeton.edu/~ste/
Find out more

**Project Wiki:** wiki.mozilla.org/Security/Contextual_Identity_Project/Containers

**User Contexts/Containers Implementation:** Bug 1191418

**OriginAttributes Implementation:** Bug 1179985

Questions?

**Github:** englehardt
**Research:** webtab.princeton.edu
**Personal:** cs.princeton.edu/~ste/