

Web Security

CS642: Computer Security



Professor Ristenpart

<http://www.cs.wisc.edu/~rist/>

rist at cs dot wisc dot edu

Liberal borrowing from Mitchell, Boneh, Stanford CS 155

Announcements

- HW3 should be posted tonight or tomorrow
- Check the web site announcements
- Check email

Web security part 1



Basic web security models

Browser security

Same-origin policy / Navigation policy

Cookies / Session handling

WWW

Tim Berners-Lee and Robert Cailliau 1990
HTTP, CERN httpd, gopher

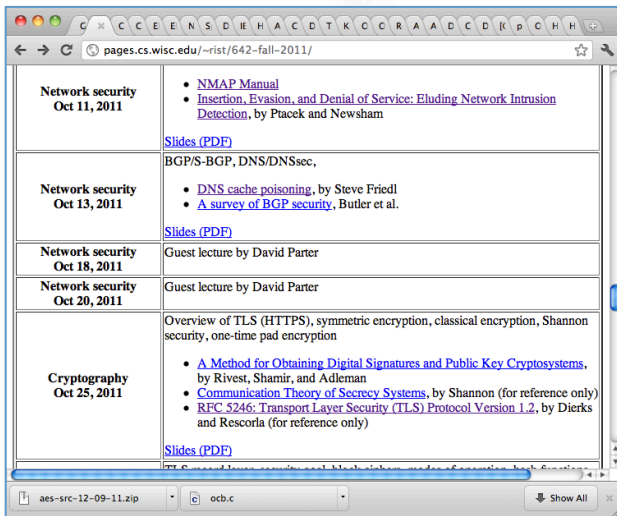
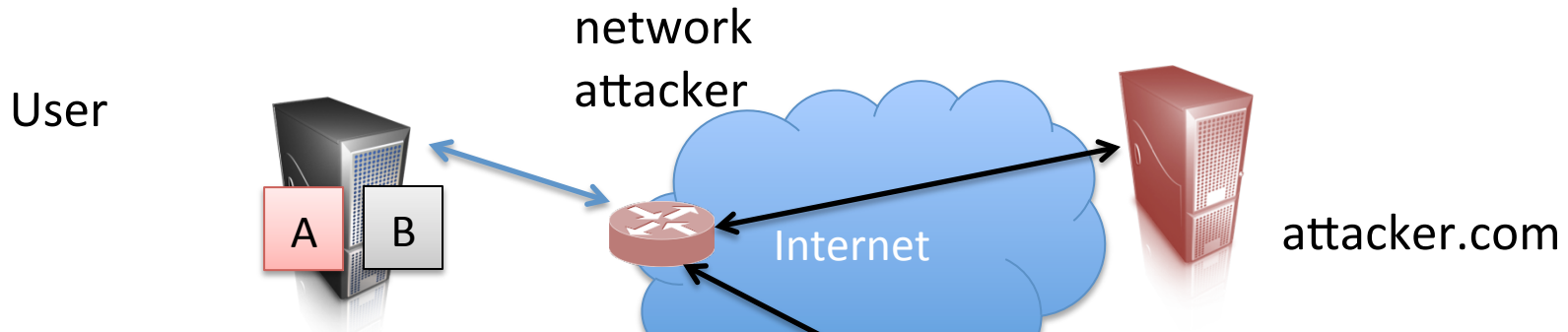
1993 Mosaic web browser (UIUC, Marc Andreessen)

1994 W3C WWW Consortium --- generate standards
Gopher started charging licensing fees
(Univ of Minnesota)

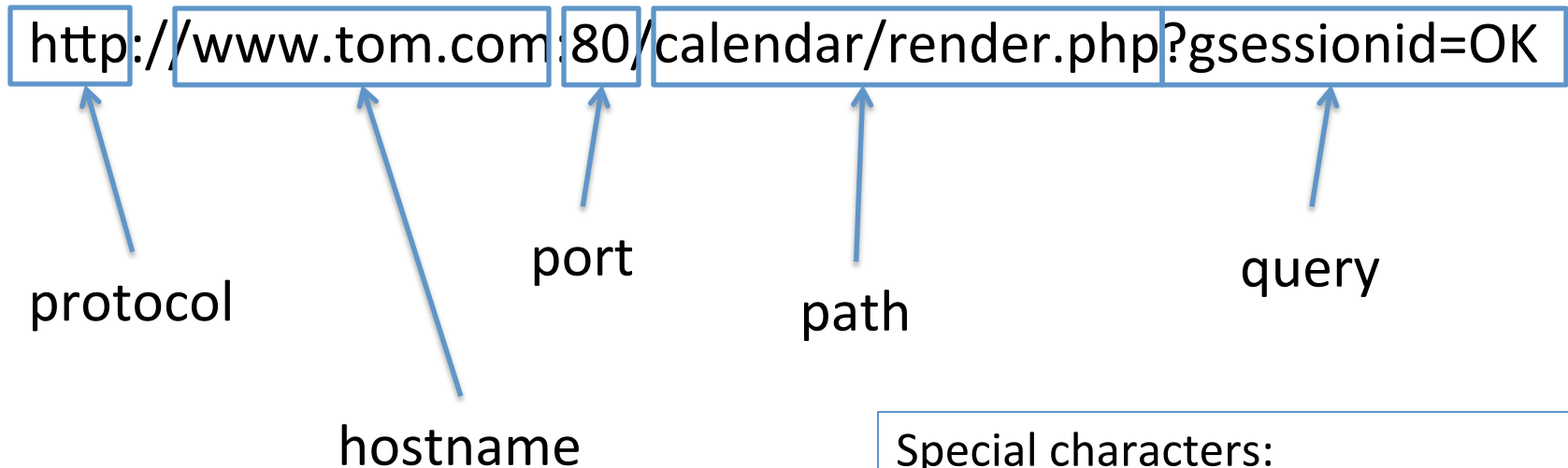
Nowdays: ecosystem of technologies

- HTTP / HTTPS
- AJAX
- PHP
- Javascript
- SQL
- Apache
- Ruby
- <http://w3schools.com/>

Threat model



Some basics of HTTP



URL's only allow ASCII-US characters.
Encode other characters:

`%0A` = newline

`%20` = space

Special characters:

`+` = space

`?` = separates URL from parameters

`%` = special characters

`/` = divides directories, subdirectories

`#` = bookmark

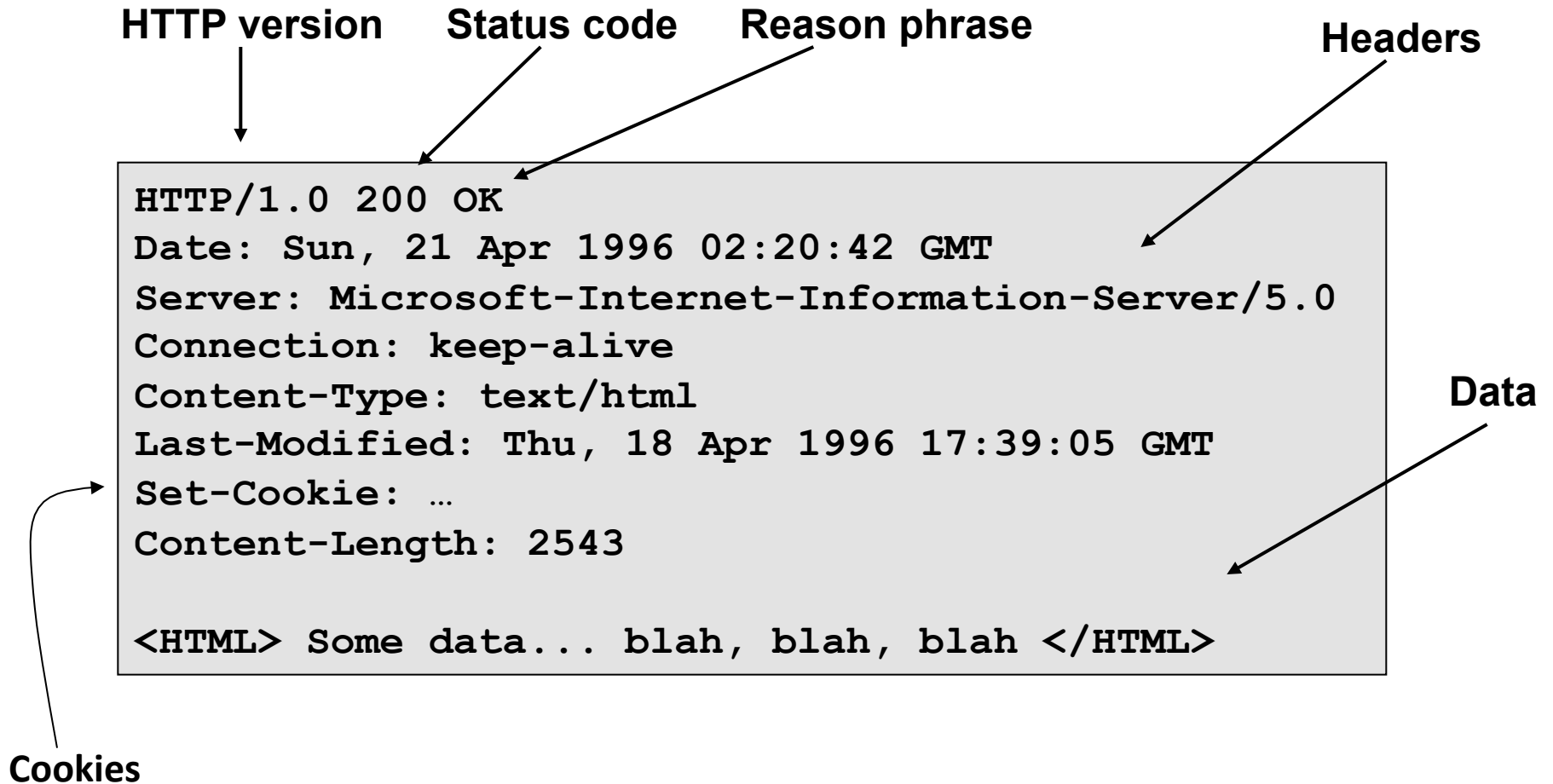
`&` = separator between parameters

HTTP Request

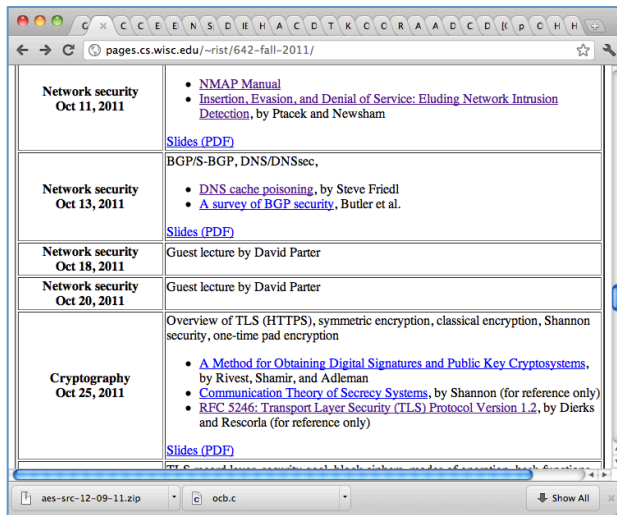


GET : no side effect POST : possible side effect

HTTP Response



Browser execution



- Each window (or tab):
 - Retrieve/load content
 - Render it
 - Process the HTML
 - Might run scripts, fetch more content, etc.
 - Respond to events
 - User actions: OnClick, OnMouseover
 - Rendering: OnLoad, OnBeforeUnload
 - Timing: setTimeout(), clearTimeout()

Web pages are not single-origin

IFrames: `<iframe src="//site.com/frame.html" > </iframe>`

Scripts: `<script src="//site.com/script.js" > </script>`

CSS:

`<link rel="stylesheet" type="text /css" href="//site/com/theme.css" />`

Objects (flash): [using swfobject.js script]

`<script>`

```
var so = new SWFObject('//site.com/flash.swf', ...);
so.addParam('allowscriptaccess', 'always');
so.write('flashdiv');
```

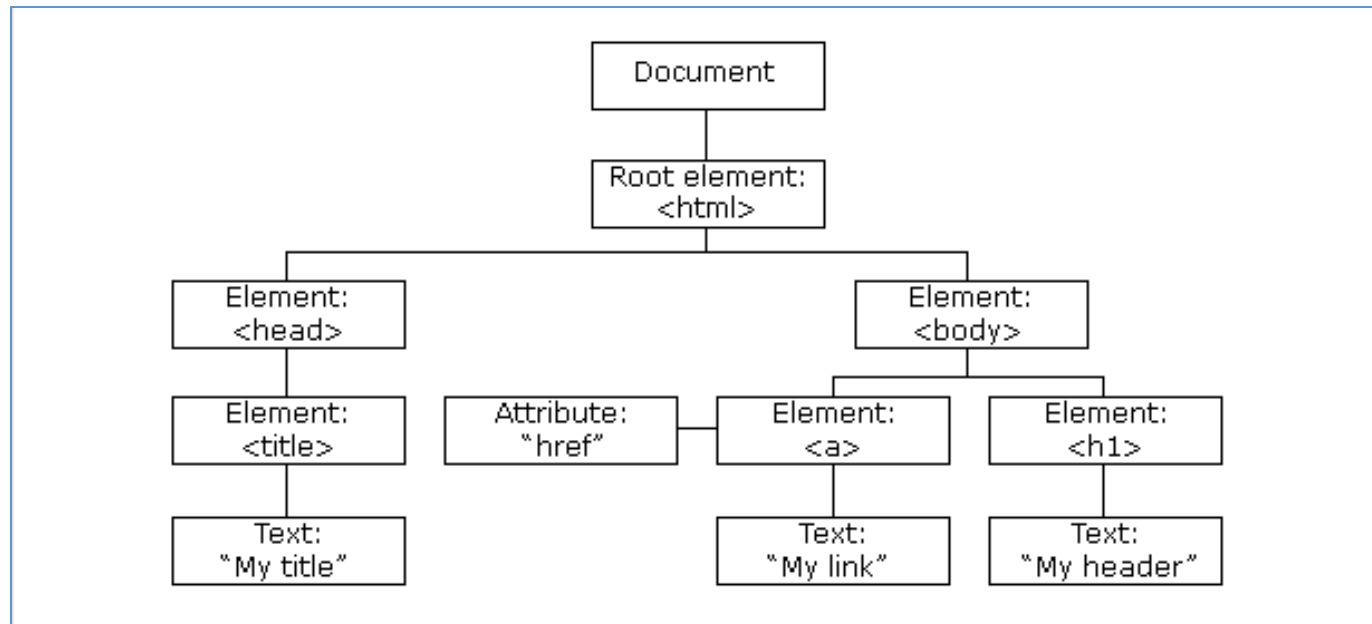
`</script>`

Document Object Model (DOM)

Object-oriented way to refer to objects in a web page

Properties: document.alinkColor, document.URL, document.forms[], document.links[], document.anchors[]

Methods: document.write(document.referrer)



From <http://w3schools.com/html/dom/default.asp>

Document Object Model (DOM)

Object-oriented way to refer to objects in a web page

Properties: `document.alinkColor`, `document.URL`,
`document.forms[]`, `document.links[]`, `document.anchors[]`

Methods: `document.write(document.referrer)`

Browser Object Model (BOM)

`window`, `document`, `frames[]`, `history`, `location`,
`navigator` (type and version of browser)

Seemingly innocuous features?

- ``
- Displays an image
- What can attacker do?

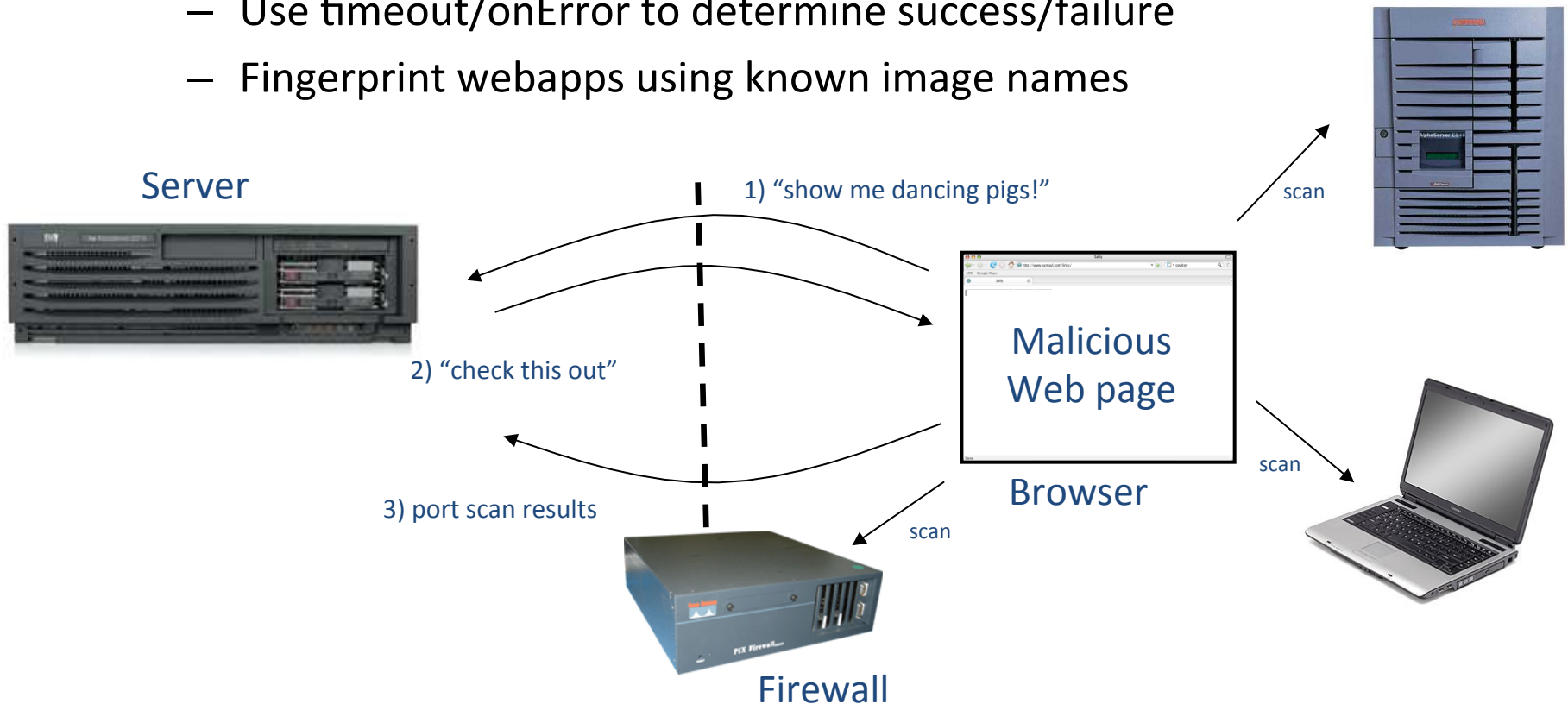


Javascript timing

```
<html><body><img id="test" style="display: none">
<script>
  var test = document.getElementById('test');
  var start = new Date();
  test.onerror = function() {
    var end = new Date();
    alert("Total time: " + (end - start));
  }
  test.src = "http://www.example.com/page.html";
</script>
</body></html>
```

Behind-firewall webapp scanning

- JavaScript can:
 - Request images from internal IP addresses
 - Example: ``
 - Use timeout/onError to determine success/failure
 - Fingerprint webapps using known image names

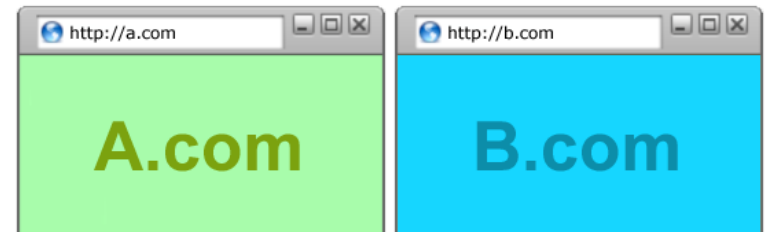


Browser security model

Should be safe to visit an attacker website



Should be safe to visit sites simultaneously



Should be safe to delegate content



Browser isolation



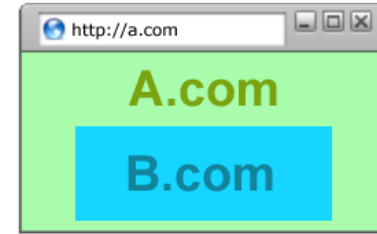
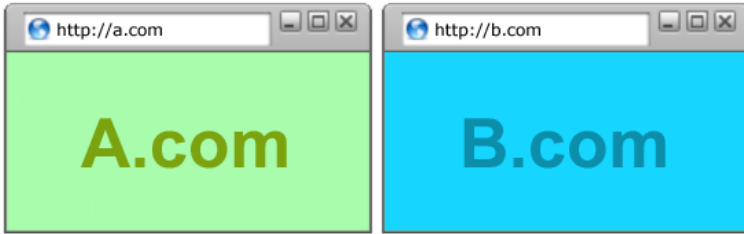
Browser is running untrusted inputs (attacker webpage)

Like all big, complex software, browser has security vulnerabilities

Browsers include “Rich Internet Applications” (RIAs) that increase attack surface:

e.g., Adobe Flash (see reading for today by Blazakis)

Malicious website exploits browser, from there system



Browser handles multiple sites, must maintain separate security contexts for each

Operating system

- Primitives
 - System calls
 - Processes
 - Disks
- Principals: Users
 - Discretionary access controls
- Vulnerabilities
 - Buffer overflows
 - root exploit
 - ...

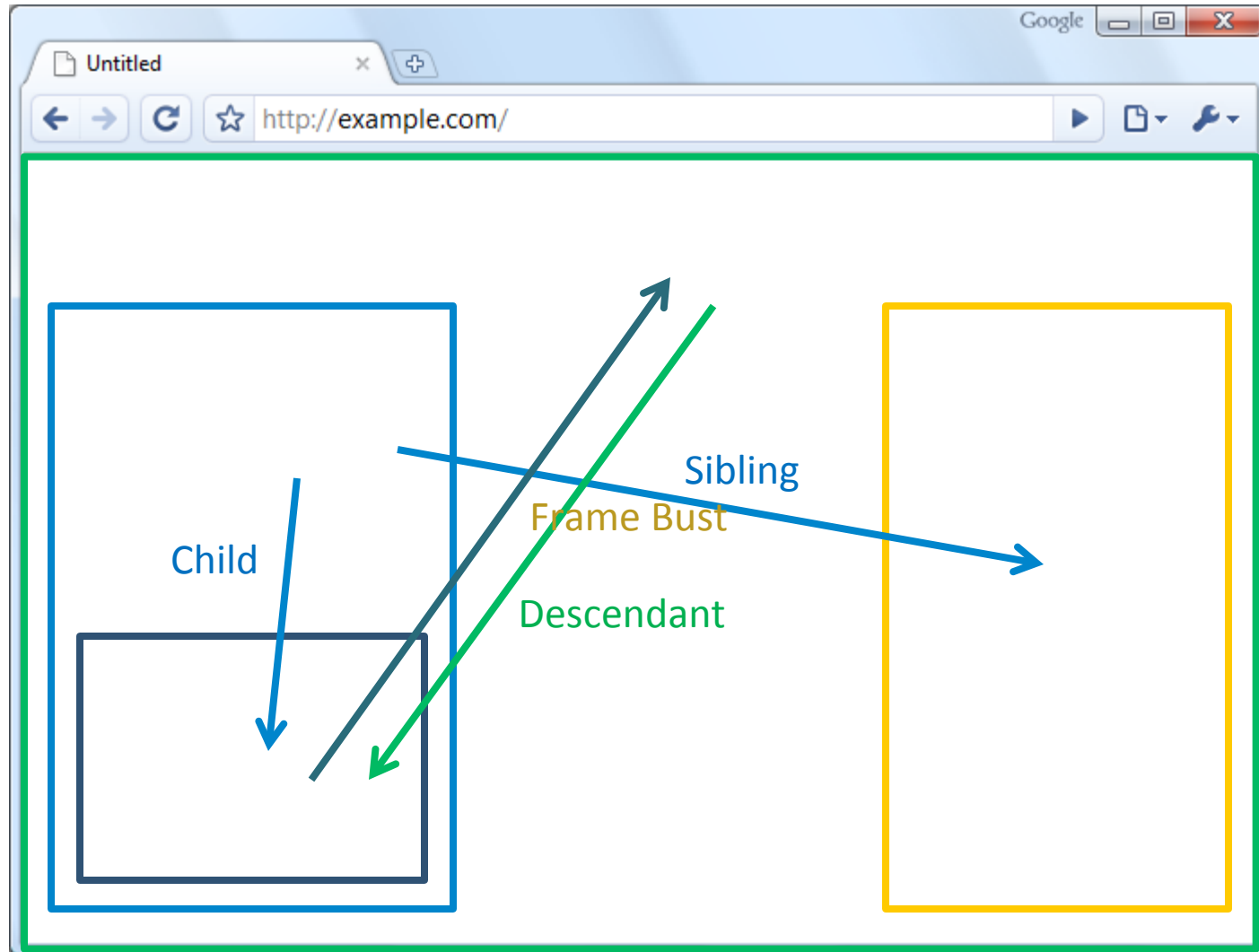
Browsers

- Primitives
 - Document object model
 - Frames
 - Cookies / local storage
- Principals: Origins
 - Mandatory access controls
- Vulnerabilities
 - Cross-site scripting (XSS)
 - Cross-site request forgery (CSRF)
 - Cache history attacks
 - ...

Same-origin policy

- Each frame of page(s) has an origin
 - protocol://host:port
 - Origin is (protocol,host,port)
- Frame can access its own origin
 - Network access, Read/write DOM, storage (cookies)
- Frame cannot access data associated with another origin

Frame relationships



Frame policies

`canScript(A,B)` and `canNavigate(A, B)`

- Permissive
 - any frame can navigate any other frame
- Child
 - only can navigate if you are parent
- Descendent
 - only can navigate if you are ancestor

Which do you think should be used?

Problems with permissive

`frames['right'].window.location="evil.com/login.html";`

Welcome to AdSense - Windows Internet Explorer

https://www.google.com/adsense/login/en_US/

Welcome to AdSense

Google AdSense

English (US) Help Center

Earn money from relevant ads on your website
Google AdSense matches ads to your site's content, and you earn money whenever your visitors click on these ads.

Sign up now >

awglogin

Existing AdSense users:
Sign in to Google AdSense with your Google account

Email:
Password:

Sign in

I cannot access my account

Garden Tips
Roses, Daisies. and more
Local florists. Same day delivery
Freshest flowers from \$10.99
www.seedsandsaplings.com

Place ads on your site

```
window.open("https://attacker.com/", "awglogin");
```

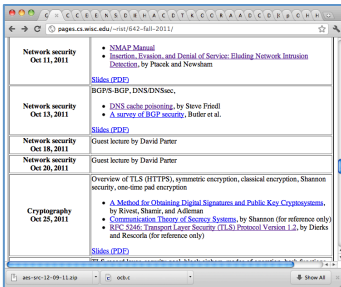
UI Redressing (Clickjacking)

The screenshot shows a Windows Internet Explorer browser window with the title "Welcome to AdSense - Windows Internet Explorer". The address bar contains the URL "https://www.google.com/adsense/login/en_US/". The page content includes the Google AdSense logo, a language dropdown set to "English (US)", and a "Help Center" link. The main heading reads "Earn money from relevant ads on your website" with a subtext: "Google AdSense matches ads to your site's content, and you earn money whenever your visitors click on them." A large blue button labeled "Do evil thing()" is overlaid on the page. Below this, there is a sign-in section for "Existing AdSense users" with fields for "Email:" and "Password:", a "Sign in" button, and a link for "I cannot access my account". An advertisement for "Roses, Daisies. and more" from "www.seedsandsaplings.com" is displayed, with a green arrow pointing to it and the text "Place ads on your site" below. The text "Overlaid frame" is written in large black font across the middle of the page.

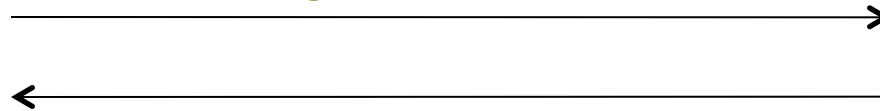
Framebusting

```
<script type="text/javascript">  
    if(top != self) top.location.replace(location);  
</script>
```

Cookies: Setting/Deleting



GET ...



HTTP Header:

Set-cookie: NAME=VALUE ;

if expires=NULL:
this session only

domain = (when to send) ;
path = (when to send)

scope

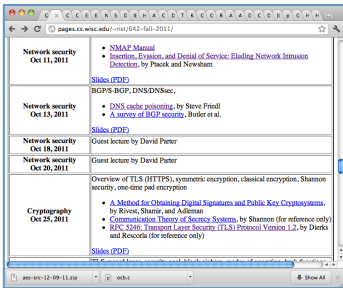
secure = (only send over SSL);
expires = (when expires) ;
HttpOnly

- Delete cookie by setting “expires” to date in past
- Default scope is domain and path of setting URL
- Client can also set cookies (Javascript)

Cookie scope rules (domain and path)

- Say we are at www.wisc.edu
 - Any non-TLD suffix can be scope:
 - allowed: www.wisc.edu or wisc.edu
 - disallowed: www2.wisc.edu or ucsd.edu
- Path can be set to anything

Cookies: reading by server



GET /url-domain/url-path

Cookie: name=value



- Browser sends all cookies such that
 - domain scope is suffix of url-domain
 - path is prefix of url-path
 - protocol is HTTPS if cookie marked "secure"

Cookie security issues

- Cookies have no integrity
 - HTTPS cookies can be overwritten by HTTP cookie (network injection)
 - Malicious clients can modify cookies
 - Shopping cart vulnerabilities
- Privacy
 - Cookies can be used to track you around the Internet
- HTTP cookies sent in clear
 - Session hijacking

ally
Do you love your bank?

Introducing
Ally IRA Online Savings Account
Rollover available with Traditional and Roth IRAs

0.89%
ANNUAL PERCENTAGE YIELD
[learn more](#)

Member
Ally Bank **FDIC**

[Send News](#). Want a reply? [Read this](#). More in the [FAQ](#). [News Forum](#) - [All Forums](#) - [Mobile](#) - [PDA](#) - [RSS Headlines](#)  [Twitter](#) 

STORIES OF NOTE

Tuesday, Nov 08, 2011

[Batman: Arkham City This Month](#)
[D: MW3 Ships](#)
[One Gold - Skyrim](#)
[Inbow 6 Patriots](#)
[AS Announcement](#)
[Battlefield 3 Ships](#)
[AV Trailer Next Week](#)
[3 MP Confirmed](#)
[Portal 2 DLC Oct 4](#)

PC Batman: Arkham City This Month [10:40 am ET] - [Share](#) - [2 Comments](#)

WBIE announces the release dates for the [delayed](#) Windows PC edition of **Batman: Arkham City**, the stealth/action sequel:

Warner Bros. Interactive Entertainment and DC Entertainment today confirmed that the Games for Windows PC version of **Batman: Arkham City** will be available in North America beginning November 22, in Australia beginning November 23, in France and Benelux beginning November 24, and in other European territories beginning November 25.



Get
fr

Answers.com Now Only With Facebook and Own Login

Posted by **timothy** on Tuesday November 08, @12:30PM
from the you-haff-been-assimilated dept.

facebook

[CptnHarlock](#) writes

"Today the registered users of [Answers.com](#) received an email informing them that the site has [ended support](#) for Yahoo, Twitter, Google, or LinkedIn as a way to sign into their site. Facebook is the sole external way left to log in. A local login and password were generated and sent by email and the old (non-Facebook) logins deactivated. Score another one for Facebook.com in the login consolidation wars."

Read the **14** comments

 [facebook](#) [google](#) [privacy](#)

ally
Introducing the
Raise Your Rate 4-Year CD

1.65%
ANNUAL PERCENTAGE YIELD
4-YEAR CD

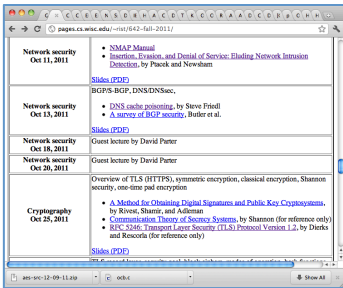
If rates go up, yours can too. Twice.

[learn more](#)

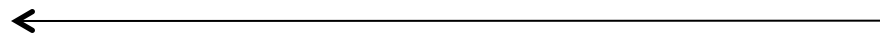
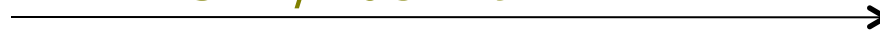
Member
Ally Bank **FDIC**

```
<script type="text/javascript">
  //
    var hint = 'mainpage';
    document.write('&lt;script type="text/javascript" src="http://ad.doubleclick.net/adj/
ostg.slashdot/pg_index_p1_leader;pg=index2;logged_in=0;tile='+dfp_tile
+';sz=728x90;u=;ord='+dfp_ord+'?'&gt;&lt;/script&gt;');
    dfp_tile++;
  //]]&gt;
&lt;/script&gt;</pre></div><div data-bbox="204 412 989 672" data-label="Text"><p>In addition to ads based on interest categories, Google allows advertisers (including Google) to show you ads based on your previous interactions online, such as visits to advertisers' websites. For example, someone who visited the website of an online sporting goods store can receive ads about special offers from that store. --- <a href="http://www.google.com/privacy/ads/">http://www.google.com/privacy/ads/</a></p></div><div data-bbox="34 727 972 832" data-label="Section-Header"><h2>Google Dominates Search Advertising With 80% Market Share Unaffected By The Rise Of Bing</h2></div><div data-bbox="38 858 83 912" data-label="Image"><img alt="ADV MEDIA PRODUCTIONS logo"/>The logo for ADV Media Productions, featuring the letters 'ADV' in a large, bold, blue font above the word 'MEDIA' in a smaller, blue font, with 'PRODUCTIONS' in a very small font below it. The entire logo is set against a black square background.</div><div data-bbox="91 855 487 880" data-label="Text"><p>Posted on June 21, 2011 by <a href="#">Advanced Media Productions</a></p></div>
```

Session handling and login



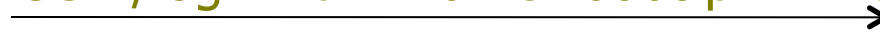
GET /index.html



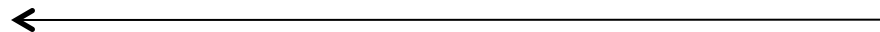
Set-Cookie: AnonSessID=134fds1431

Protocol
is HTTPS.
Elsewhere
just HTTP

POST /login.html?name=bob&pw=12345



Cookie: AnonSessID=134fds1431



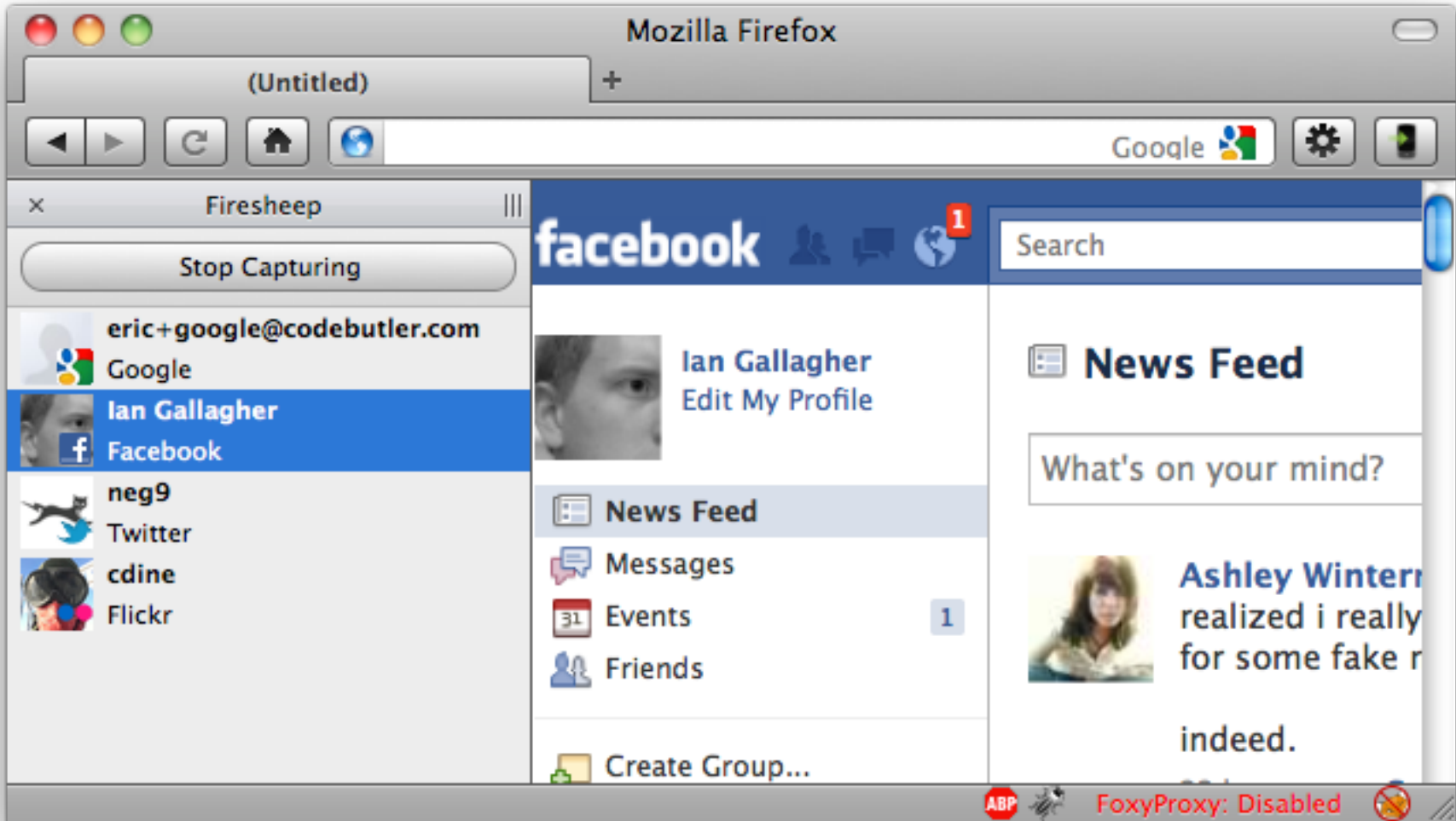
Set-Cookie: SessID=83431Adf

GET /account.html



Cookie: SessID=83431Adf

Session Hijacking



From <http://codebutler.com/firesheep>

Towards preventing hijacking

- Use encryption when setting session cookies
- $SessID = Enc(K, info)$ where :
 - K is server-side secret key
 - Enc is Encrypt-then-MAC encryption scheme
 - info contains:
 - user id
 - expiration time
 - other data
- Server should record if user logs out
- Does this prevent Firesheep hijacking?
 - include in data machine-specific information
 - turn on HTTPS always