







Enforcing Content Security By Default within Web Browsers



Christoph Kerschbaumer

Content Security Checks

-  ***File Access Permission***
-  ***Same Origin Policy***
-  ***Cross Origin Resource Sharing***
-  ***Mixed Content Blocking***
-  ***Content Security Policy***
-  ***Subresource Integrity***
-  ***...***

Content Security Checks

 ***File Access Permission***

 ***Same Origin Policy***

 ***Cross Origin Resource Sharing***

 ***Mixed Content Blocking***

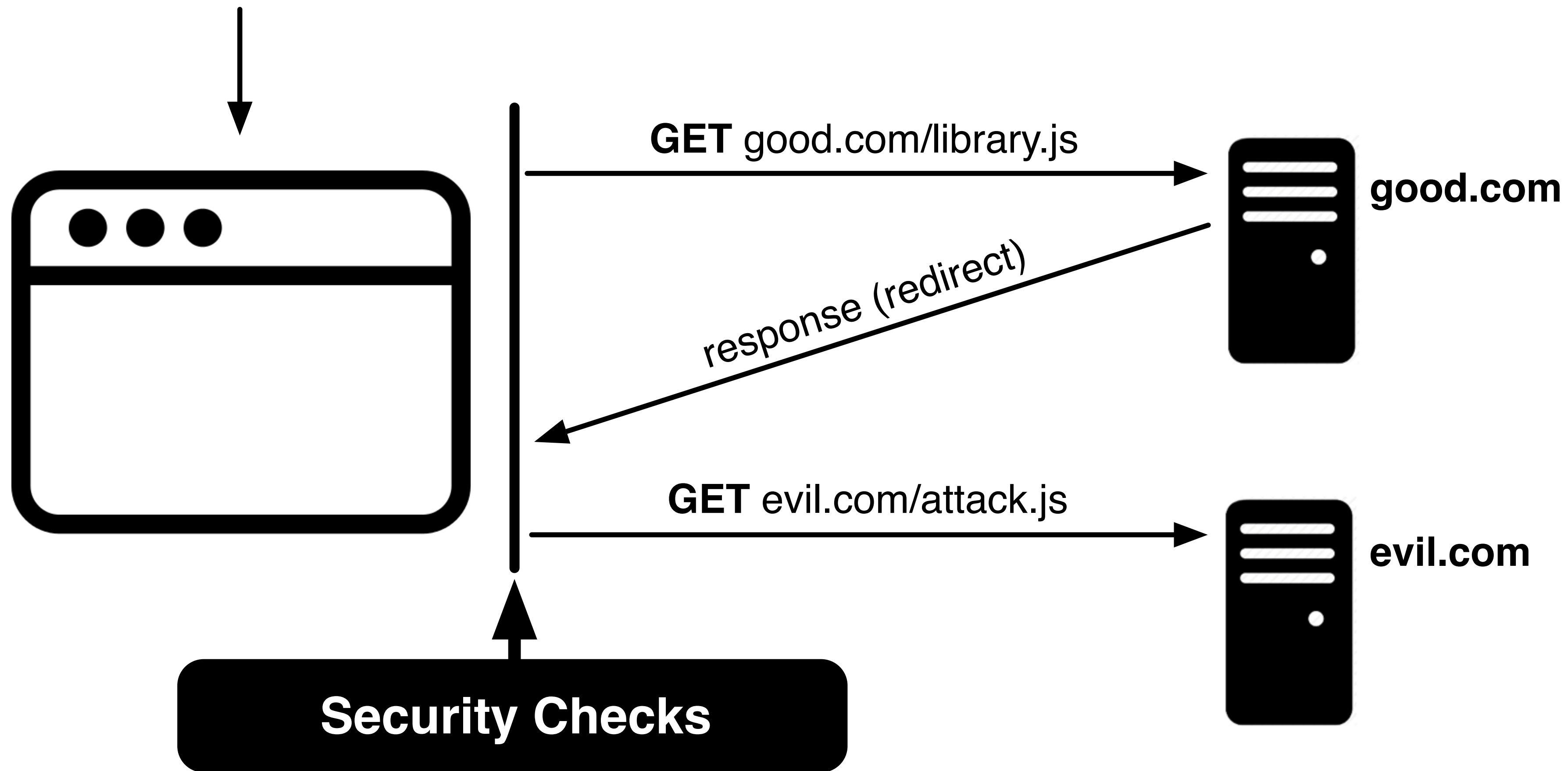
  ***Content Security Policy***

 ***Subresource Integrity***

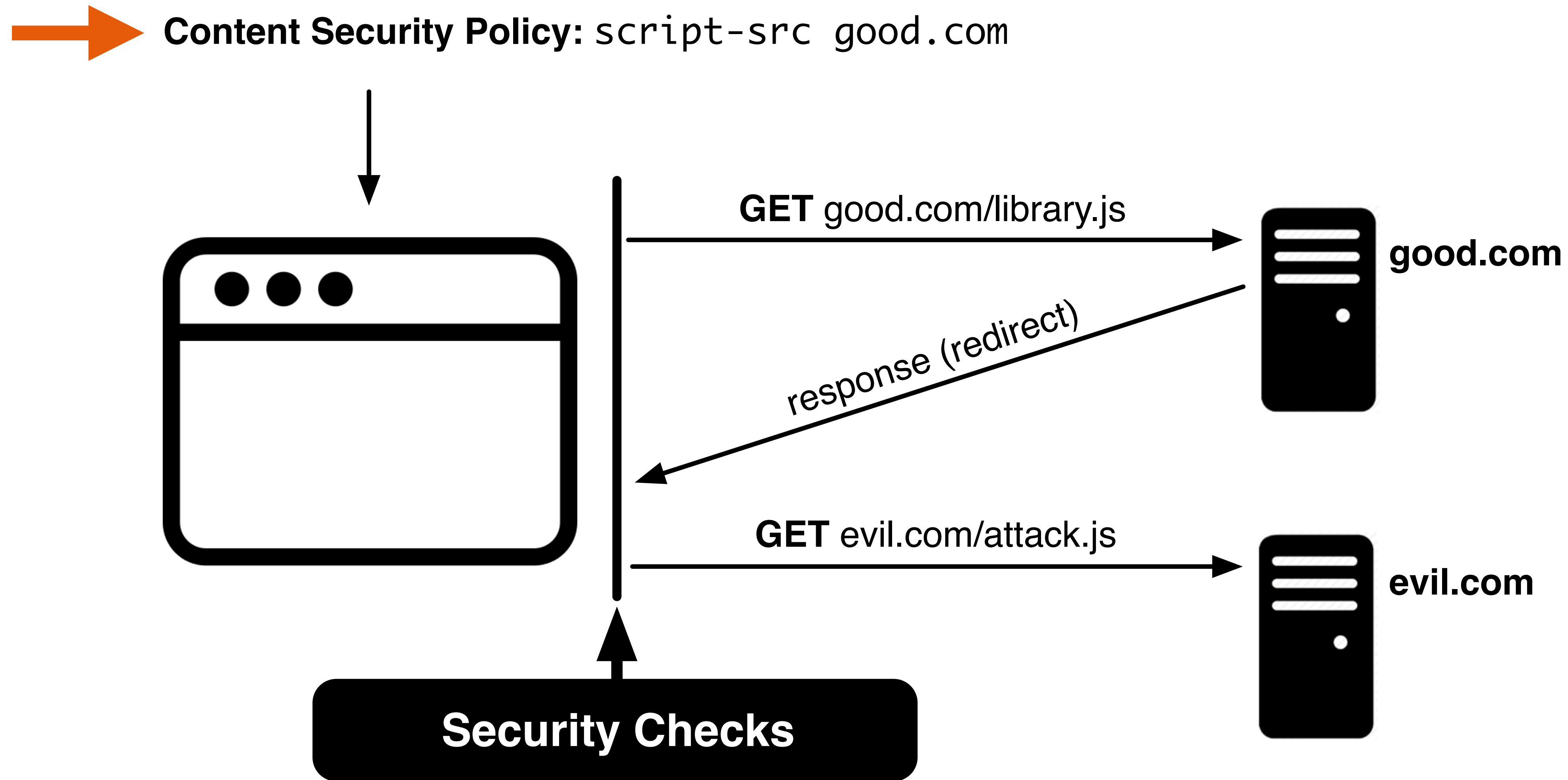
 ***...***

Performing Content Security Checks

Content Security Policy: `script-src good.com`

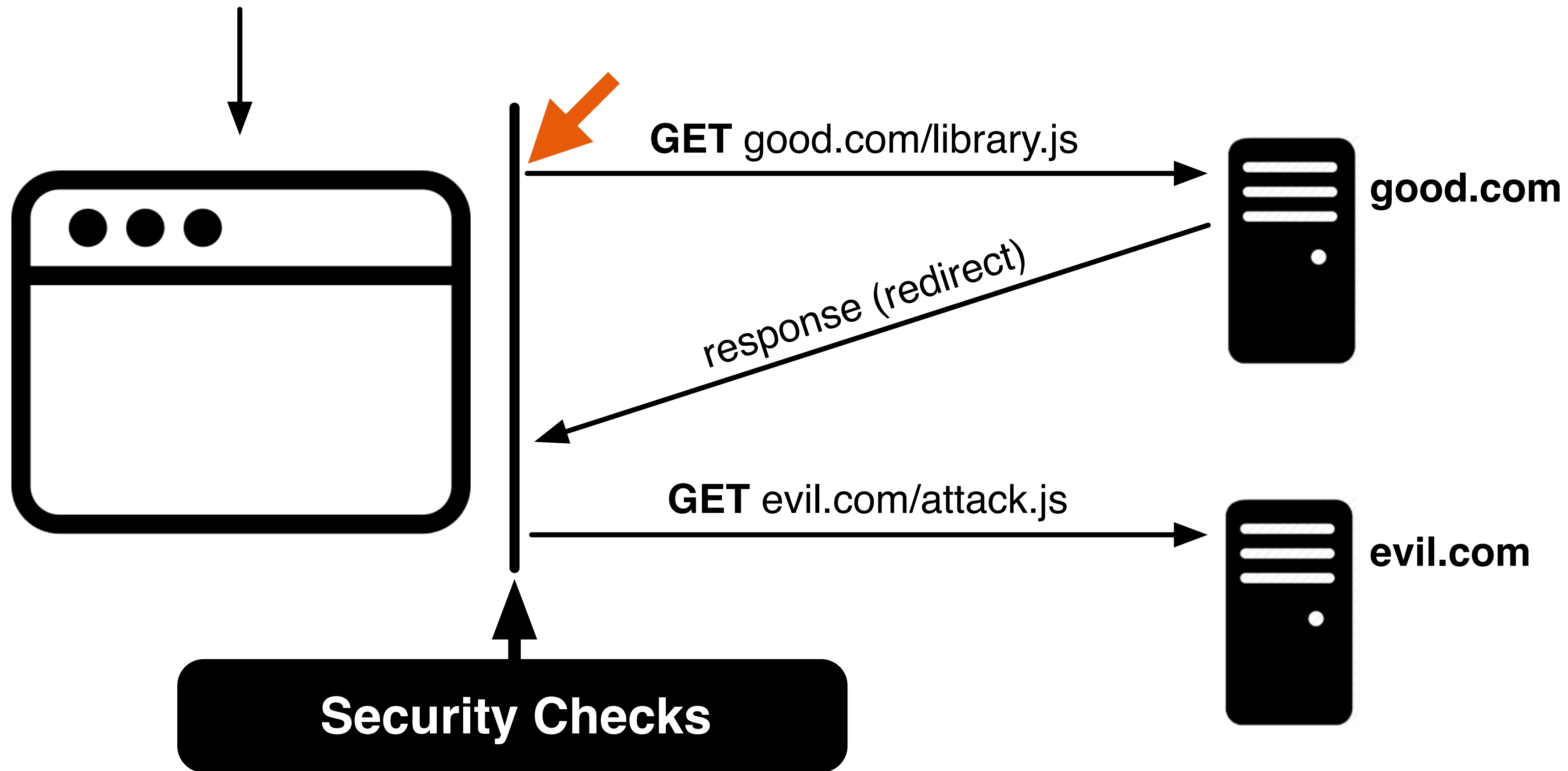


Performing Content Security Checks



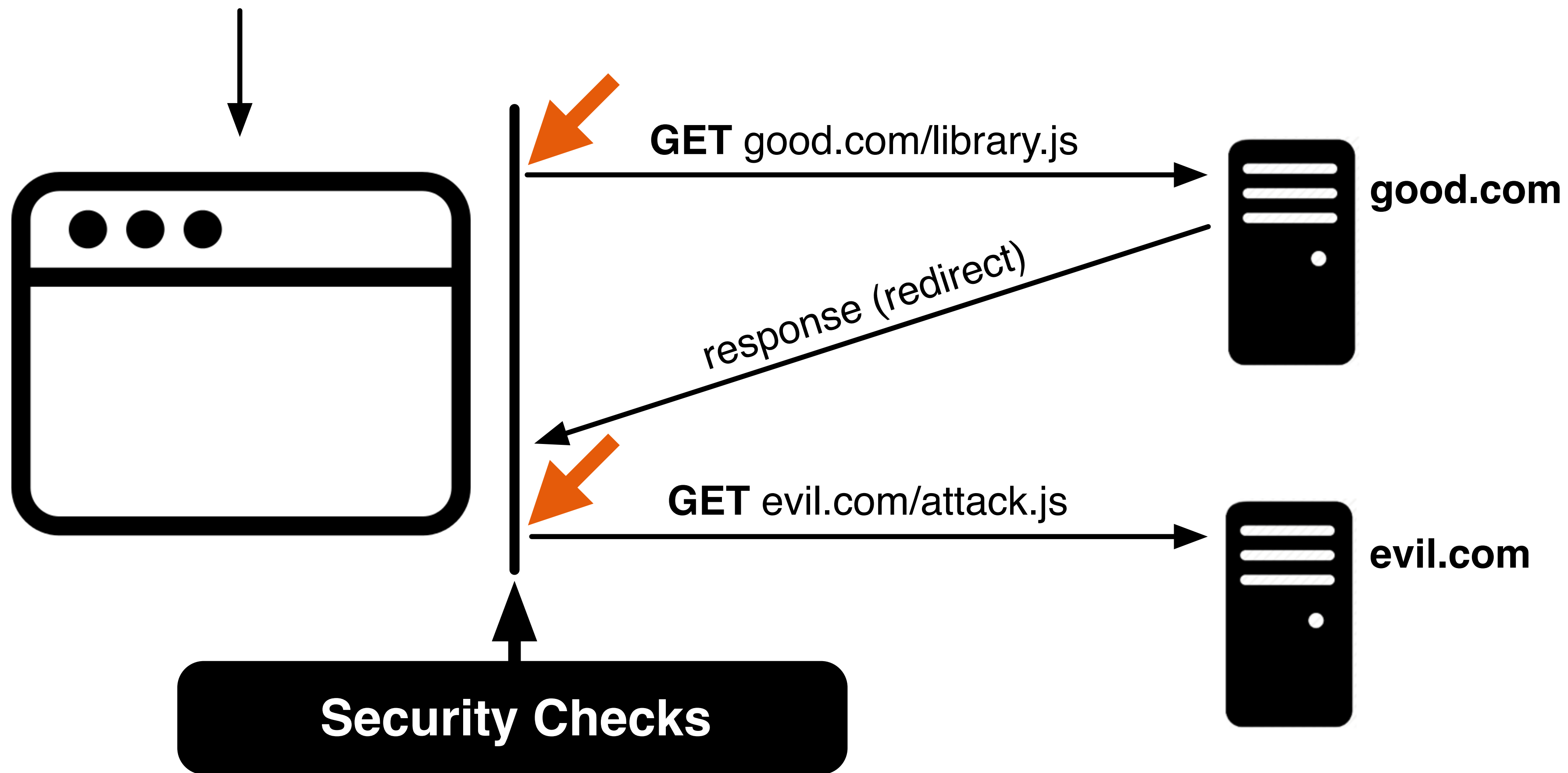
Performing Content Security Checks

Content Security Policy: `script-src good.com`



Performing Content Security Checks

Content Security Policy: `script-src good.com`



Terminology

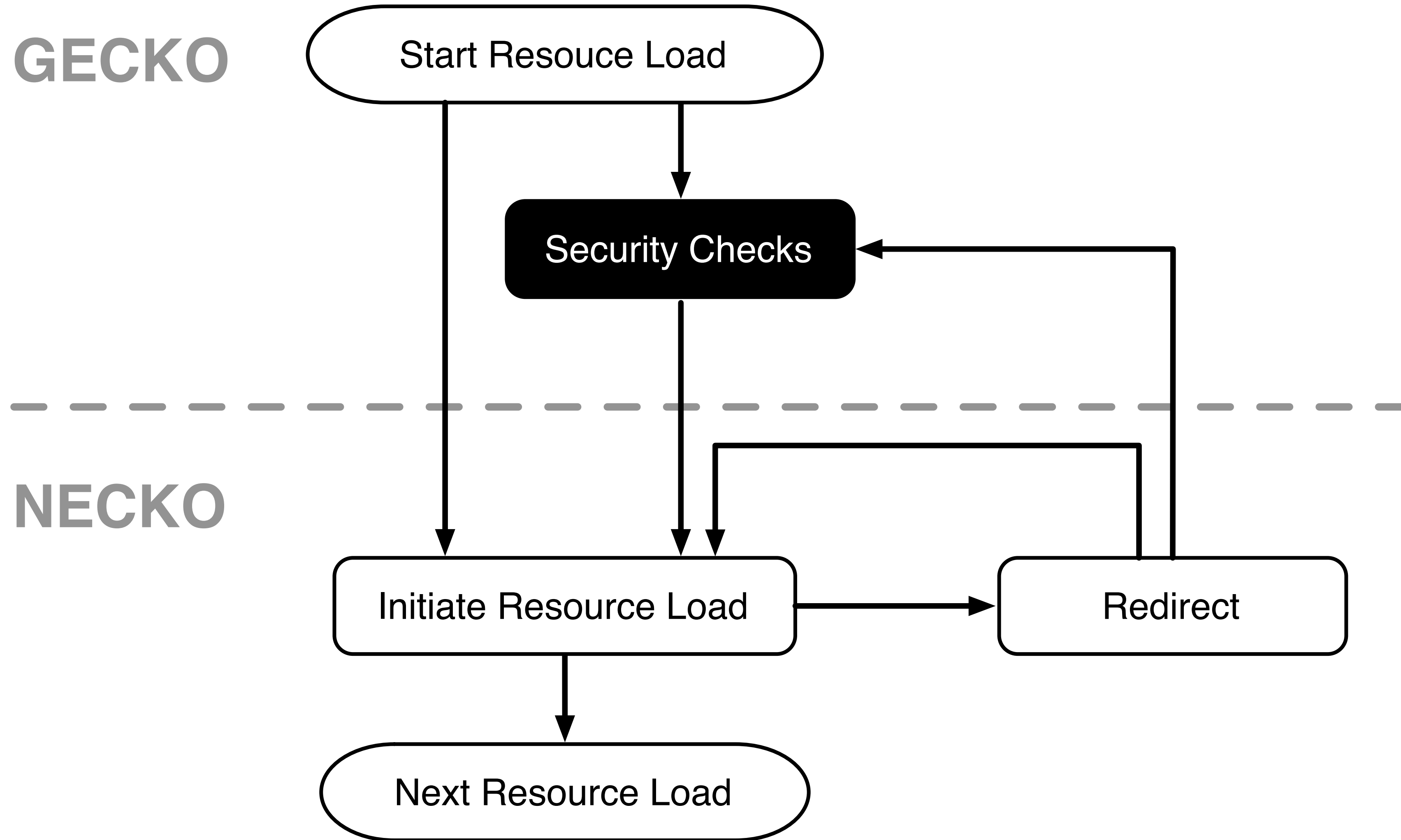
GECKO

*Layout Engine within Firefox
renders web content, such as (HTML, JS, CSS, etc.)*

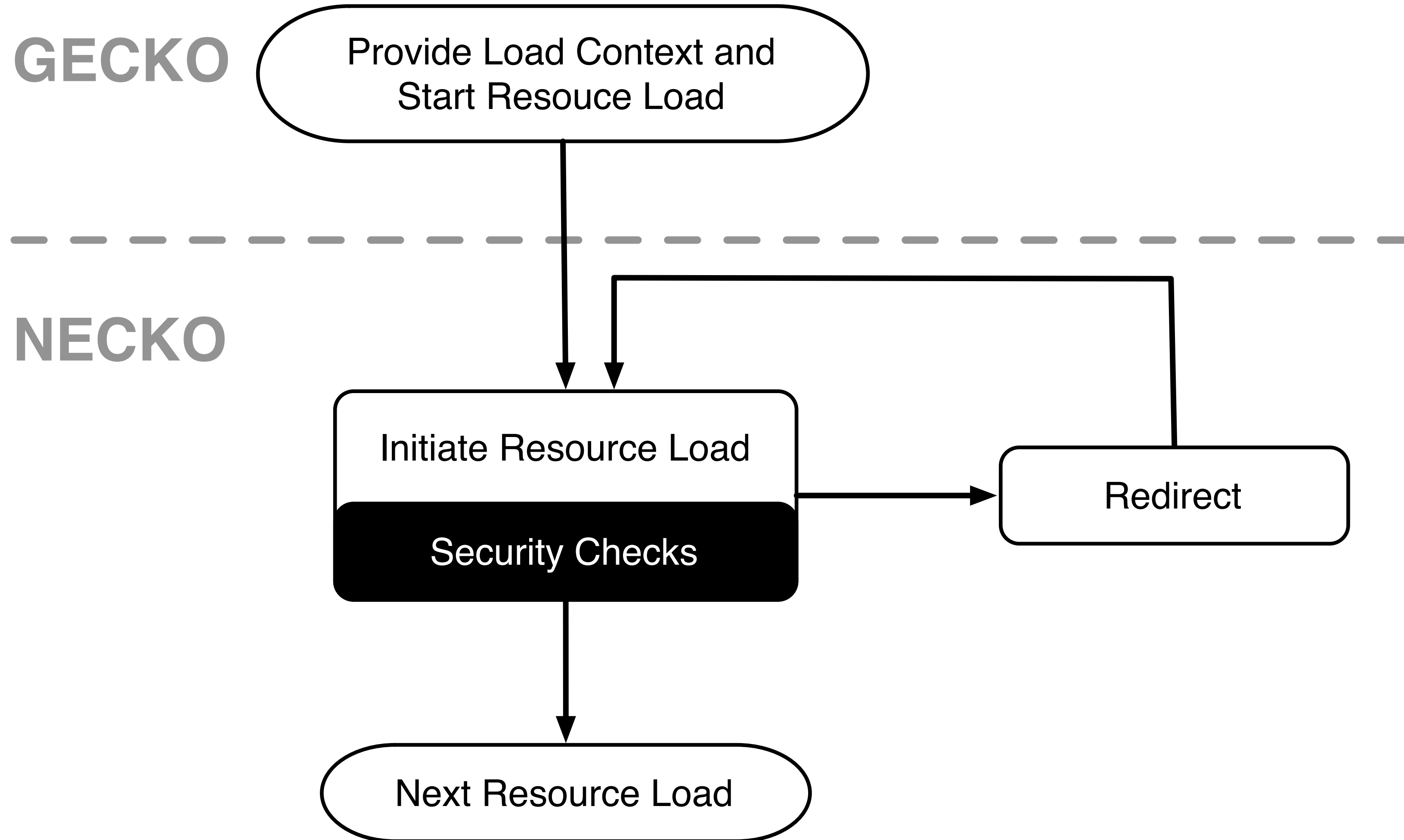
NECKO

*Network Library within Firefox
loads resources over the internet*

Performing Security Checks Historically



Performing Security Checks By Default



Performing Security Checks By Default

GECKO

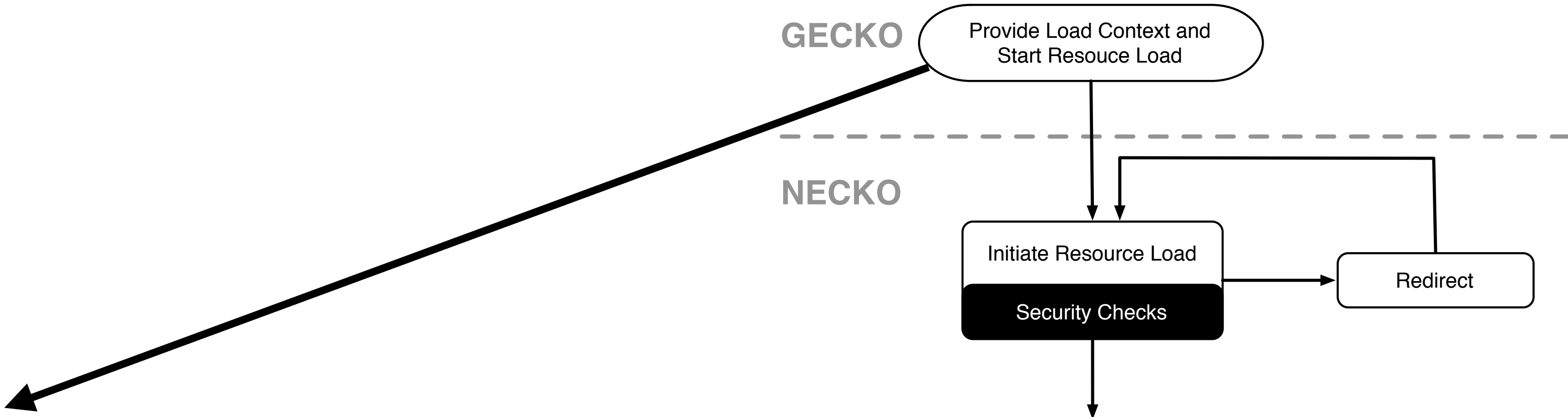
Provide Load Context and Start Resource Load

NECKO

Initiate Resource Load
Security Checks

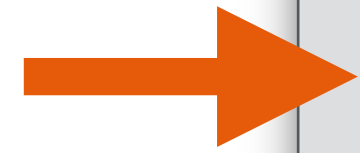
Redirect

Next Resource Load



```
LoadInfo {  
  Principal* loadingPrincipal;  
  ContentPolicyType contentPolicyType;  
  SecurityFlags securityFlags;  
};
```

Providing Load Context



```
LoadInfo {  
  Principal* loadingPrincipal;  
  ContentPolicyType contentPolicyType;  
  SecurityFlags securityFlags;  
};
```

LoadingPrincipal

***Content
Principal***

***Presents Security Context of web content
reflects origin of that content***

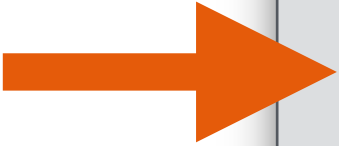
***System
Principal***

***Reflects Security Context of the system
bypasses all security checks***

***Null
Principal***

***Reflects Sandboxed security context
only same origin with itself***

Providing Load Context



```
LoadInfo {  
    Principal* loadingPrincipal;  
    ContentPolicyType contentPolicyType;  
    SecurityFlags securityFlags;  
};
```

ContentPolicyType

SCRIPT

FONT

VIDEO

IMAGE

IFRAME

FAVICON

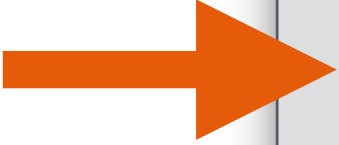
STYLE

AUDIO

...

Providing Load Context

```
LoadInfo {  
    Principal* loadingPrincipal;  
    ContentPolicyType contentPolicyType;  
    SecurityFlags securityFlags;  
};
```



SecurityFlags

REQUIRE_SAME_ORIGIN_DATA_INHERITS

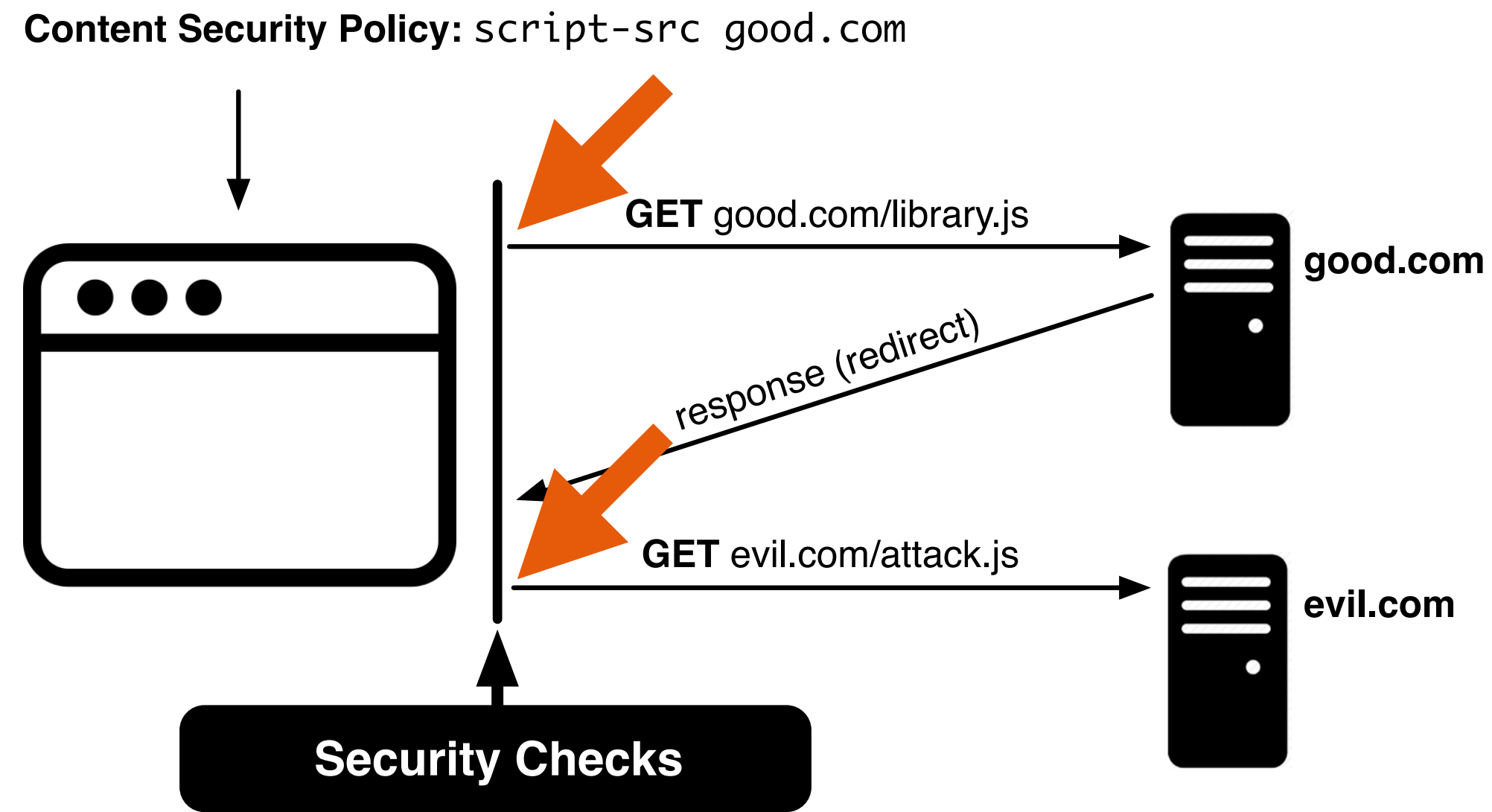
REQUIRE_SAME_ORIGIN_DATA_IS_BLOCKED

ALLOW_CROSS_ORIGIN_DATA_INHERITS

ALLOW_CROSS_ORIGIN_DATA_IS_NULL

REQUIRE_CORS_DATA_INHERITS

Performing Content Security Checks



```
LoadInfo {  
  Principal* loadingPrincipal          = https://good.com  
  ContentPolicyType contentPolicyType = TYPE_SCRIPT;  
  SecurityFlags securityFlags         = ALLOW_CROSS_ORIGIN;  
};
```






Server Side Redirects

<i>HTTP Response Status Codes incl. Description</i>	<i>%</i>	<i>%</i>
2xx Success		61.86
200 OK	61.86	
3xx Redirection		11.82
301 Moved Permanently	0.76	
302 Found	7.66	
307 Temporary Redirect	3.33	
308 Permanent Redirect	0.07	
xxx Other responses		26.32
4xx, 5xx, ...	26.32	

Server Side Redirects

<i>HTTP Response Status Codes incl. Description</i>	<i>%</i>	<i>%</i>
2xx Success		61.86
200 OK	61.86	
3xx Redirection		11.82 ←
301 Moved Permanently	0.76	
302 Found	7.66	
307 Temporary Redirect	3.33	
308 Permanent Redirect	0.07	
xxx Other responses		26.32
4xx, 5xx, ...	26.32	

Engineering Effort

-  ***100+ updated network loads***
-  ***400+ tests that verify network loads***
-  ***20 months***
-  ***One Engineer full time***
-  ***Dozens of reviewers***

Engineering Effort



 ***100+ updated network loads***

 ***400+ tests that verify network loads***

 ***20 months***

 ***One Engineer full time***

 ***Dozens of reviewers***

  ***518 changesets***

  ***126,322 lines of code (hg diff -p -U 8)***

  ***3,500 man hours***

Thank You



Mozilla
Firefox

Christoph Kerschbaumer