COOKIE SECURITY

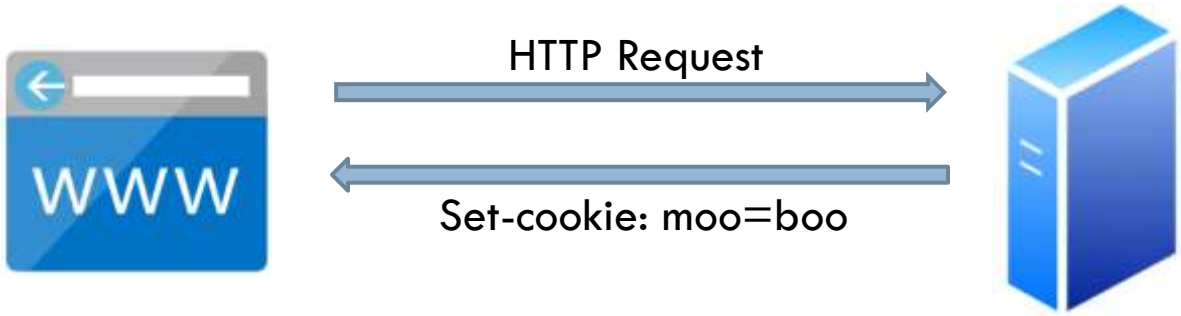
Stephen Schaub

Cookie Attributes

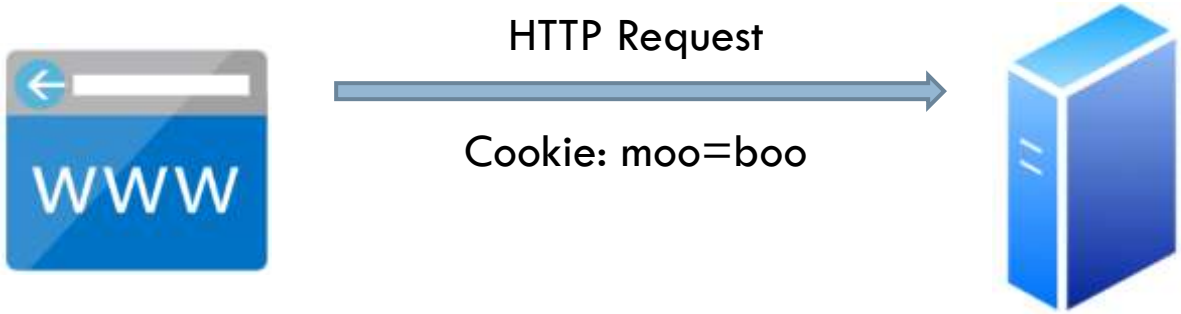
- A cookie has the following attributes:
  - name
  - value
  - domain (domain name that sent the cookie)
  - path (path prefix for which cookie will be sent)
  - expiration
  - secure (true/false)
  - http only (true/false)
  - same site (None, Lax, Strict)

Recall Basic Cookie Behavior

- Browser sends request to server
  - Server sends response with Set-cookie: header



- Browser sends a subsequent request to same server, including cookie



Cookie Security Basics

- Treat a cookie as just another piece of input from the user
  - Why can you not assume that it came from your application?
- Assume that the cookie may have been modified (or even created) by the user
  - Validate the cookie data
  - Don't store sensitive data in cookies without using encryption

Cookie Domain and Path attributes

- Consider a cookie C and an HTTP request *R*
  - R = http(s)://domain/path
- A browser sends a cookie C with an HTTP request *R* only if C matches the domain and path of *R*
  - C.domain = R.domain (subdomains are allowed if domain specified in Set-cookie)
  - C.path matches left-hand portion of R.path
- Consider a cookie with a domain=**cnn.com** and a path=**/auth**:
  - Sent to http://cnn.com/auth/login
  - Not sent to http://cnn.com/top-stories
  - Perhaps sent to http://www.cnn.com/auth

Secure Cookies

- A “secure” cookie is one whose secure attribute is “true”
  - Browsers send secure cookies only for https: URL’s
- Note that “secure” cookies can be manipulated or generated by user, just like other cookies
- They are “secure” because they are transmitted in an encrypted HTTP request
- Any session- or authentication-related cookies should have their “secure” attribute set to true

Examples

- http://moo.com/boo
- https://moo.com/boo/soo
- http://moo.com/moo/soo

Cookie Name	Domain	Path	Secure
cookie1	moo.com	/boo	true
cookie2	moo.com	/soo	false
cookie3	moo.com	/	true
cookie4	boo.com	/boo	true

Third Party Cookies

- A web page can load images and other resources from other ("third-party") domains
- Cookies originating from other domains are called "Cross-site" or "Third-party" cookies
- The **samesite** cookie attribute determines whether a browser will include certain cookies in requests for third-party resources

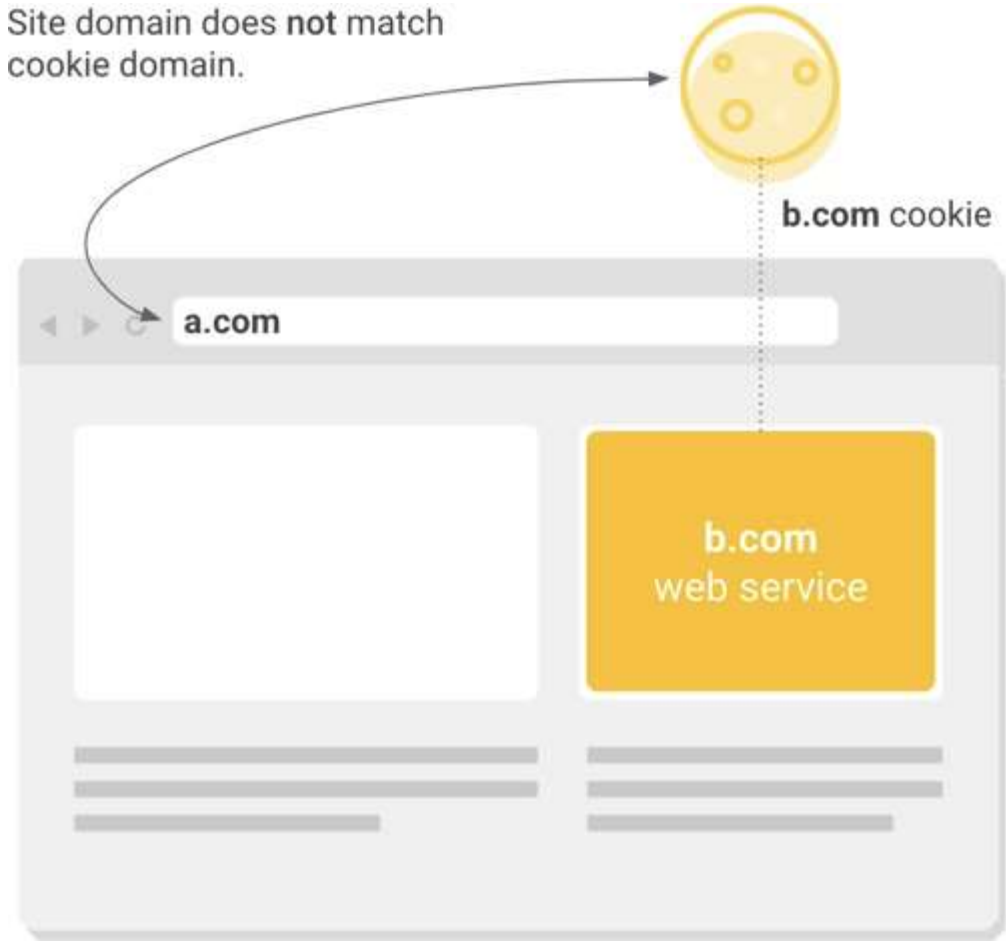


Image from https://blog.chromium.org/2019/10/developers-get-ready-for-new.html

Setting Cookie Properties

- See http://expressjs.com/en/4x/api.html#res.cookie

Further Reading

- https://blog.chromium.org/2019/10/developers-get-ready-for-new.html
  - SameSite property