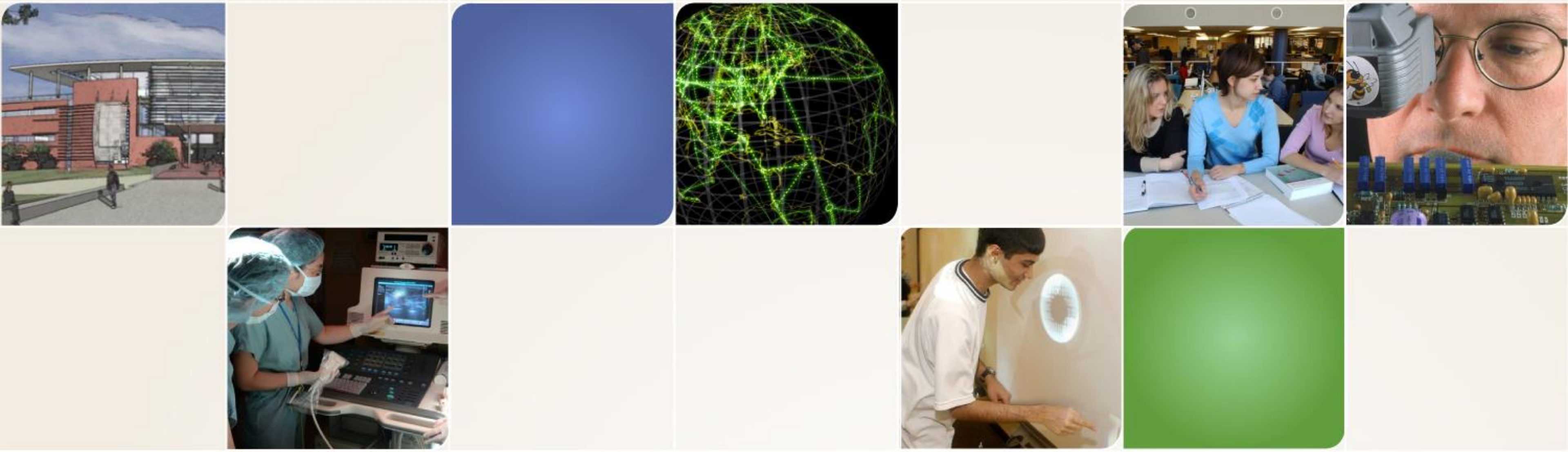


Web Session Management Best Practices

By: Keith Watson
CoC Information Security Manager

Georgia Tech College of Computing

What we will be talking about today

- What is state
- Why HTTP based services need state
- How session hijacking works
- Session hijacking demonstration using Cookie Cadger
- Best practices for protecting yourself
- Best practices for protecting services
- Where to get additional information

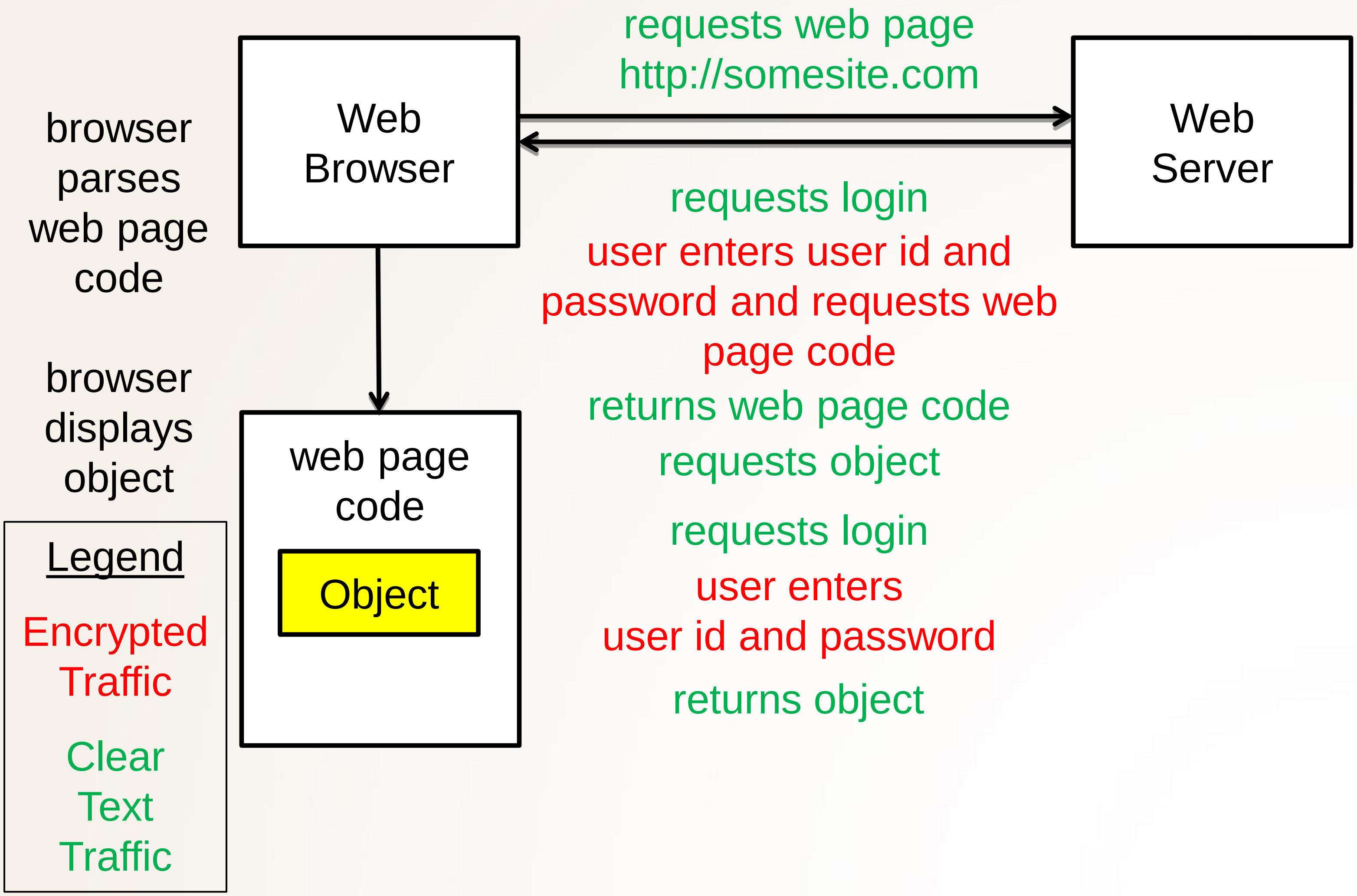
What is state?

- A stateless protocol is one that treats each transaction as unrelated to previous transactions
- HTTP by design is a stateless protocol

Why HTTP based services need state

- Any service that ties to a user’s identity needs to have state
  - Online banking
  - Web shopping
  - Social networking
  - Webmail
- Otherwise there is no way to associate each transaction with the user

Example of HTTP service **without** state



Web Browser

Web Server

requests web page http://somesite.com

browser parses web page code

requests login

user enters user id and password and requests web page code

returns web page code

browser displays object

web page code

Object

requests object

requests login

user enters user id and password

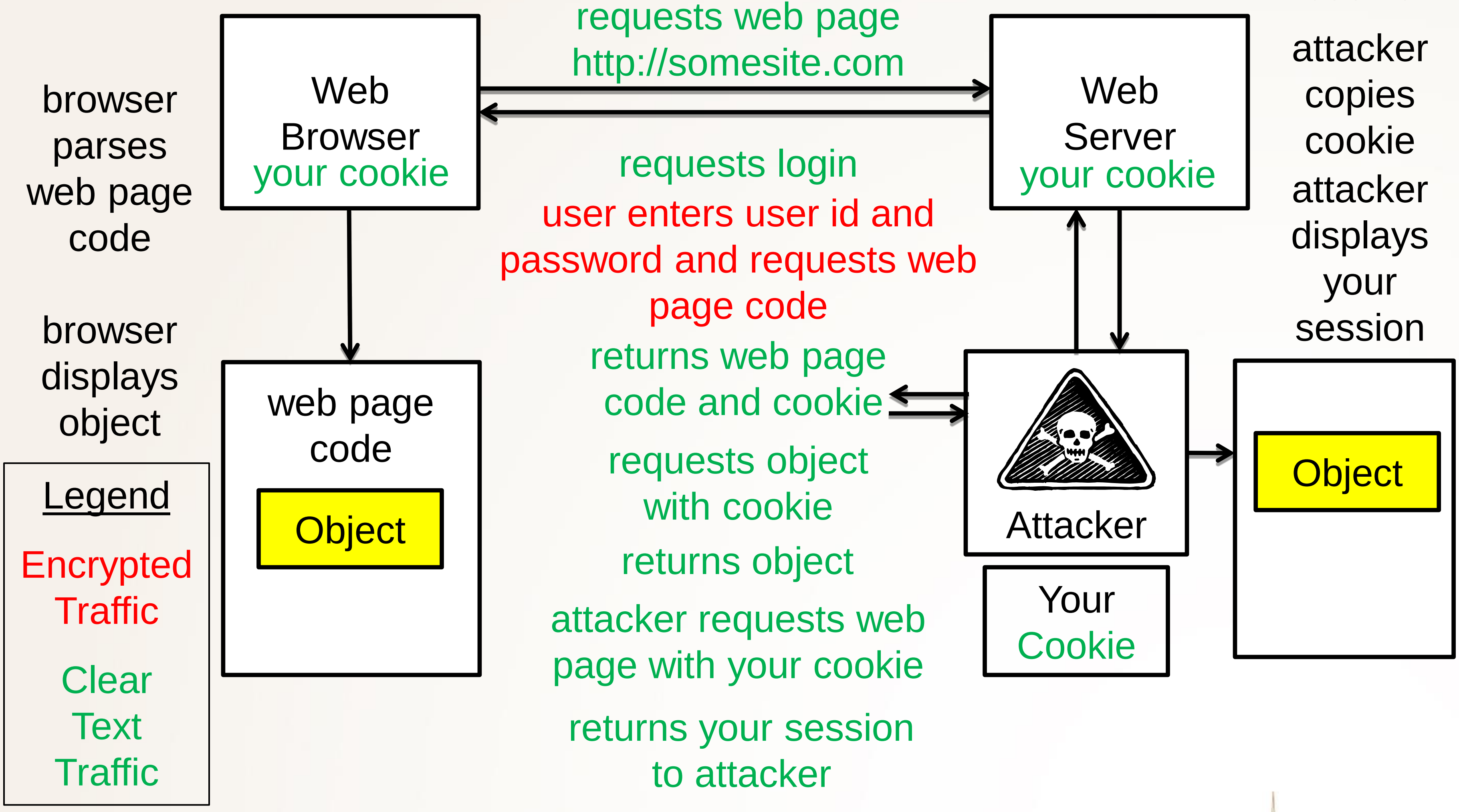
returns object

Legend

Encrypted Traffic

Clear Text Traffic

How session hijacking works



browser parses web page code

browser displays object

Legend

Encrypted Traffic

Clear Text Traffic

Web Browser
your cookie

web page code

Object

requests web page http://somesite.com

requests login

user enters user id and password and requests web page code

returns web page code and cookie

requests object with cookie

returns object

attacker requests web page with your cookie

returns your session to attacker

Web Server
your cookie

Attacker

Your Cookie

Object

attacker sees cookie

attacker copies cookie

attacker displays your session

Session hijacking demonstration

COOKIE CADGER

- Developed by Matthew Sullivan at Iowa State University

- Presented at DerbyCon 2012
- Is an: "Auditing tool for Wi-Fi or wired Ethernet connections" (also described as a replacement for Firesheep)
- Written in Java so it runs on Microsoft Windows, Linux, and OS X.

Best practices for protecting yourself

- Configure your profile to always use HTTPS
- Use fully qualified HTTPS URLs
  - you will be susceptible to a man in the middle attack if you use browser auto-complete or browse to the HTTP version of the site first and surf jacking after connecting to the secure site
  - Use Firebug add-on for Firefox to view cookie attributes

Best practices for protecting yourself contd.

- Use NoScript and/or HTTPS Everywhere add-ons for Firefox to force HTTPS and secure cookie attribute for sites that don’t have an HTTPS security option (no tool available for forcing HTTPOnly cookie attribute).

Best practices for protecting services

- Configure your web site to be secure
  - Use HTTPS
  - Don’t use mixed content on secure sites
  - Set the following cookie attributes
    - secure
    - HTTPOnly
    - Domain and Path
    - Expire and Max-Age
  - Test your site with Qualys® SSL Labs

Best practices for protecting services contd.

- OWASP - Session Management Cheat Sheet
- OWASP - Transport Layer Protection Cheat Sheet
- OWASP - Reviewing Code for Session Integrity issues
- OWASP - Testing for cookies attributes

Georgia Tech College of Computing

Best practices for protecting services contd.

- RFC6265 - [HTTP State Management Mechanism]

Resources

- This Presentation

  http://www.cc.gatech.edu/~krwatson
- OWASP - The Open Web Application Security Project

  https://www.owasp.org/
- OWASP Top Ten

  https://www.owasp.org/index.php/Top_Ten

Resources contd.

- Stateless Protocol

  https://en.wikipedia.org/wiki/Stateless_protocol

- HTTP Protocol

  https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

- Session Hijacking

  https://en.wikipedia.org/wiki/Session_hijacking

Resources contd.

- Cookie Cadger
  https://www.cookiecadger.com/
- DerbyCon
  https://www.derbycon.com/
- Information technology security audit
  https://en.wikipedia.org/wiki/Information_technology_security_audit

Georgia Tech College of Computing

Resources contd.

- Wi-Fi

  https://en.wikipedia.org/wiki/Wi-Fi
- Ethernet

  https://en.wikipedia.org/wiki/Ethernet
- Firesheep

  https://en.wikipedia.org/wiki/Firesheep
- Java

  https://en.wikipedia.org/wiki/Java_%28programming_language%29

Resources contd.

- Microsoft Windows
  https://en.wikipedia.org/wiki/Microsoft_Windows
- Linux
  https://en.wikipedia.org/wiki/Linux_distribution
- OS X
  https://en.wikipedia.org/wiki/OS_X
- HTTPS Protocol
  https://en.wikipedia.org/wiki/HTTP_Secure

Resources contd.

- URL (Uniform Resource Locator)

  https://en.wikipedia.org/wiki/Uniform_Resource_Locator

- Man in the middle attack (MITM)

  https://en.wikipedia.org/wiki/Man-in-the-middle_attack

- Surf jacking

  http://enablesecurity.com/2008/08/11/surf-jack-https-will-not-save-you/

Resources contd.

- Firebug add-on for Firefox

  https://addons.mozilla.org/en-US/firefox/addon/firebug/

- Firefox web browser

  https://www.mozilla.org/

- HTTP Cookie

  https://en.wikipedia.org/wiki/HTTP_cookie

Georgia Tech College of Computing

Resources contd.

- Cookie attributes

  https://en.wikipedia.org/wiki/HTTP_cookie#Cookie_attributes

- NoScript add-on for Firefox

  https://addons.mozilla.org/en-US/firefox/addon/noscript/

- HTTPS Everywhere add-on for Firefox

  https://www.eff.org/https-everywhere/

Resources contd.

- Secure cookie attribute

  https://www.owasp.org/index.php/SecureFlag
- HTTPOnly cookie attribute

  https://www.owasp.org/index.php/HttpOnly
- Domain and Path cookie attributes

  https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Domain_and_Path_Attributes

Resources contd.

- Expire and Max-Age cookie attributes

  https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Expire_and_Max-Age_Attributes

- Qualys® SSL Labs

  https://www.ssllabs.com/ssltest/

Resources contd.

- OWASP Session Management Cheat Sheet

  https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

- OWASP Transport Layer Protection Cheat Sheet

  https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Resources contd.

- OWASP Reviewing Code for Session Integrity issues

  https://www.owasp.org/index.php/Reviewing_Code_for_Session_Integrity_issues

- OWASP Testing for cookies attributes

  https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

Resources contd.

- RFC6265 HTTP State Management Mechanism

  https://tools.ietf.org/html/rfc6265

Resources contd.

- Contact

  Keith R. Watson

  CoC Information Security Manager

  http://www.cc.gatech.edu/~krwatson

  krwatson@cc.gatech.edu

  (404) 385-7401