

CS4001 – Trust, Risk, & Security

By: Keith Watson
CoC Information Security Manager



What we will be talking about today

- Trust, risk and security.
- How do **you** measure trust
- Choose a side
- An example of the epic failure of trust - session hijacking, Firesheep demonstration
- Stop being a victim, protect yourself
- Is it ethical or even legal
- Where to get additional information



What is trust?

- Trust – Your belief in the positive actions of a person, entity, process, or device (especially when no one is watching)
- Trust doesn't guarantee results it only predicts a **positive** outcome
- Society is built on a fabric of trust (or perceived trust)



What is risk?

- Risk - the potential that trust will lead to a negative outcome
- Risk does not guarantee failure but only predicts a **negative** outcome
- Risk = (probability of failure) x (harm)
- Risk mitigation is a contingency plan for failed trust



What is security?

- Security – actions taken to protect against risk and violation of trust
- Perfect security does not exist
- Security doesn't happen by itself
- Security takes no effort to get wrong and takes hard work to get right



How do you measure trust and risk?

- People have a natural predilection to trust
- We make trust and risk decisions based on emotion and not reason (peer pressure, oxytocin)
- We are vulnerable to anyone willing to violate trust
- Willingness to violate trust = (perceived reward) / (probability of being caught x possible consequences)



What will **you** do?

- Will you uphold trust or destroy it?
- Protect yourself (security)
 - Detect
 - Monitor
 - Respond
- Be trustworthy to others
- Require your friends to be trust worthy
- Require vendors to be trust worthy (vote with your wallet)



An example of the epic failure of trust

- Vendors have improperly handled web site [session management](#)
- The public (that's you) has done virtually nothing to protect them selves or hold vendors accountable
- Result - Bad guys are compromising your data with impunity and the only one paying the price is you



It all starts with state. What is it?

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

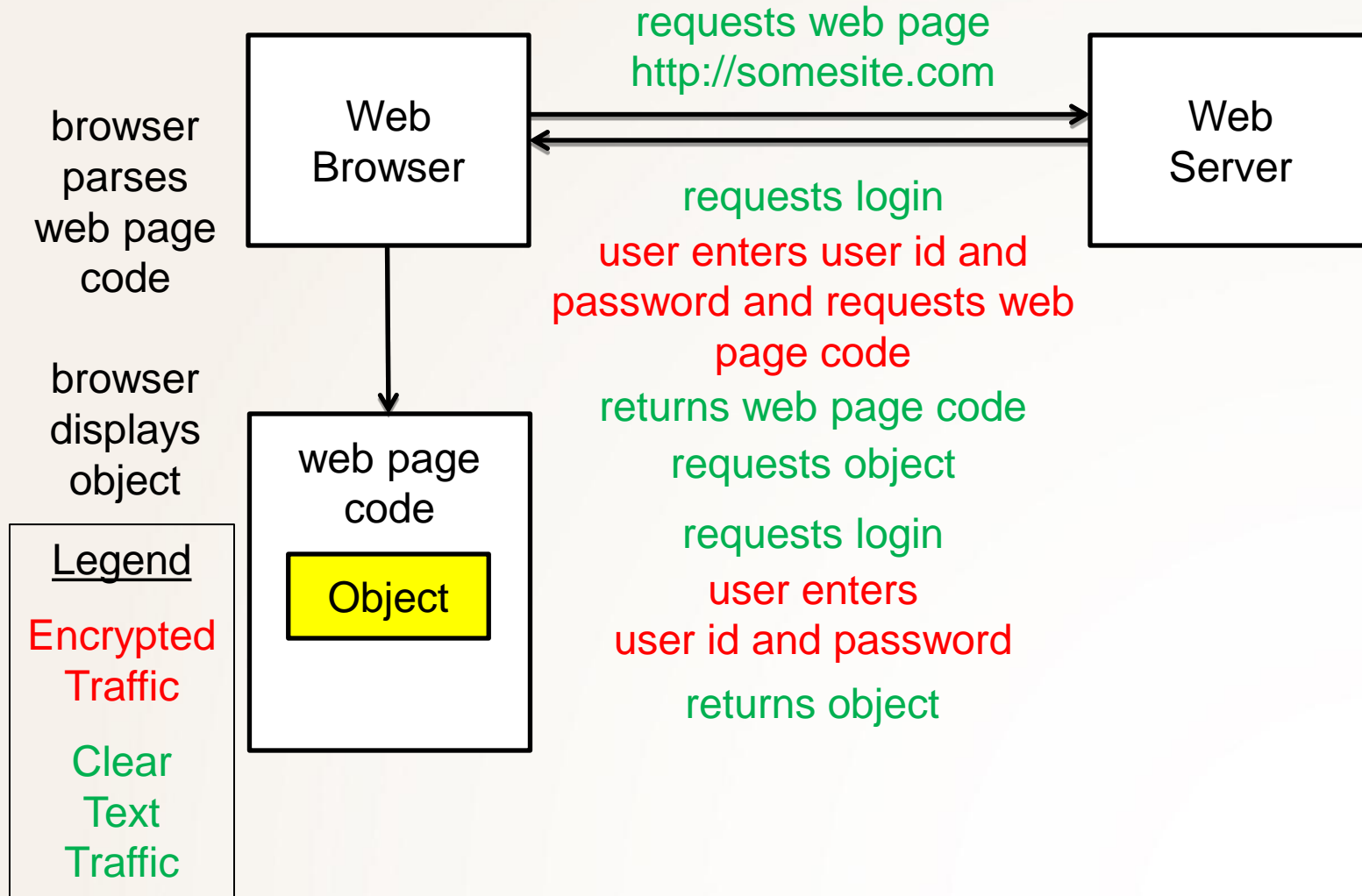


Why HTTP based services need state (session management)

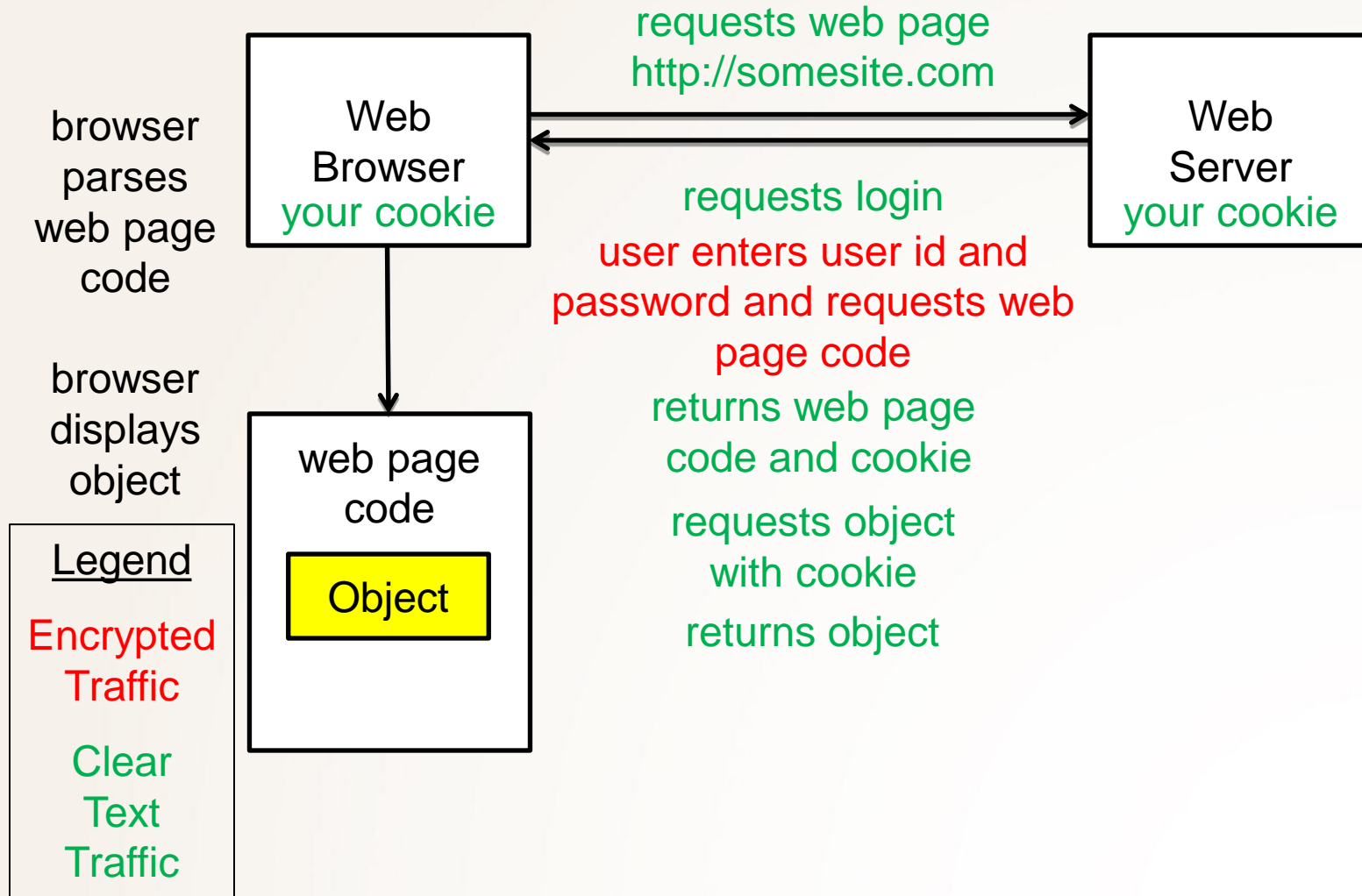
- Any service that ties to a user's identity needs to have state
 - Online banking
 - Web shopping
 - Social networking
 - Webmail
- Otherwise there is no way to associate each transaction with the user



Example of HTTP service **without** state

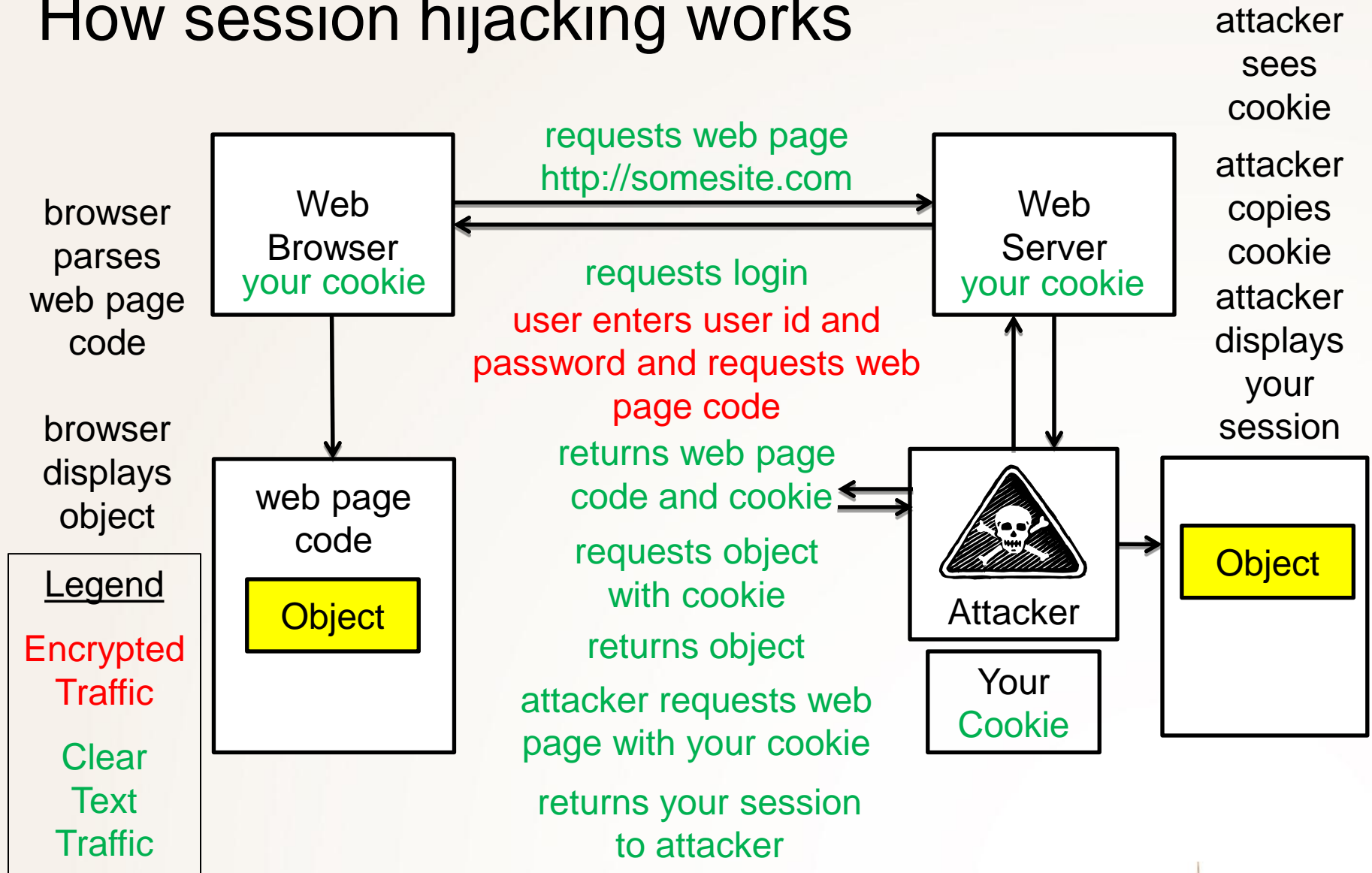


Example of HTTP service with state





How session hijacking works





Saving state with cookies – It's not new

- Cookies were the first method of saving state
 - Invented by Lou Montulli in 1994 while working for Netscape
 - Internet Explorer began supporting cookies in 1995
 - In 1996 the IETF recognized cookies as a significant privacy and security threat
 - Jan 2003 – Session Management added to OWASP Top 10



Session hijacking (sidejacking) tools

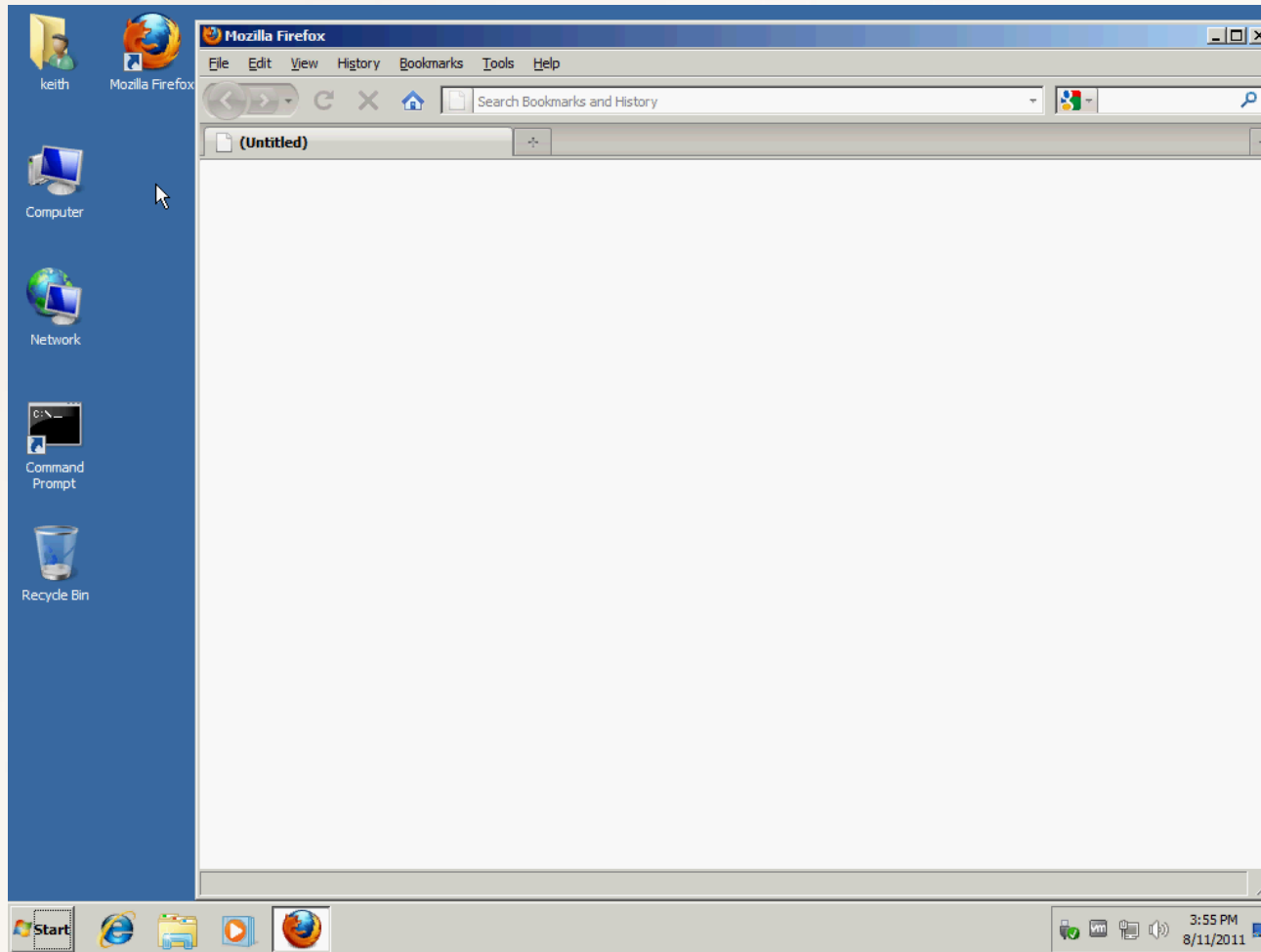
- [CookieMonster](#)
- [Edit Cookies](#)
- [FBConTroller](#)
- [Hamster & Ferret](#)
- [py-cookieJsInjection](#)
- [FaceNiff](#) ([Android](#))
- [DroidSheep](#) ([Android](#), includes [ARP Spoof](#))
- [Firesheep](#)



Why is it suddenly a big deal

- The tools for session hijacking were difficult to install and use
- Most service providers ignored the problem
- [Firesheep](#) released at [Toorcon](#), Oct. 2010
(a tool my grandmother could install and use)
- Mass media feeding frenzy (the perfect storm)
- Service providers finally took “some” action

How easy is it to install Firesheep?





Firesheep demonstration





How to protect yourself

- 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
- If you connect to an HTTP site while using an HTTPS site you are susceptible to [Surf Jacking](#)
 - use [NoScript](#) or [HTTPS Everywhere](#) to force secure cookies



How to protect yourself contd.

- Configure your profile to always use HTTPS
 - Facebook
 - [Enable Browse Facebook on a secure connection \(https\) when possible](#)
 - Gmail
 - [Always use https](#)



How to protect yourself contd.

- Configure your profile to always use HTTPS
 - Twitter – login and session are https (http no longer an option)
 - LinkedIn
 - [When possible, use a secure connection \(https\) to browse LinkedIn](#)



How to protect yourself contd.

- Force HTTPS with a plugin
 - [HTTPS Everywhere](#) ([Firefox](#) Add-On)
 - [Force-TLS](#) (Firefox Add-On)
 - [ForceHTTPS](#) (Firefox Add-On)
 - [NoScript](#) (Firefox Add-On)
 - [Use HTTPS](#) (Chrome Plugin)
 - [Fidelio](#) (Chrome Plugin)



How to protect yourself contd.

- Use a [VPN](#) (Virtual Private Network)
- Use an encrypted [anonymizer](#) or [proxy](#) (there are caveats)
 - [TOR](#) (The Onion Routing project)
 - [Want Tor to really work?](#)
 - [JonDonym](#)
 - [JAP](#) (JonDonym Anonymous Proxy)
 - [I2P](#)



Demand vendors protect you

- Configure their web site to be secure
 - Use [HTTPS](#)
 - Set the [cookie secure flag](#)
 - Use [One Time Cookies](#)
 - [Slaying Firesheep](#) (cookie management)
 - OWASP Top 10 2010-[A3-Broken Authentication and Session Management](#)
 - OWASP Top 10 2010-[A9-Insufficient Transport Layer Protection](#)



Is it ethical to create a hacking tools?

- What are the ethics related to releasing a tool like Firesheep?
 - Full disclosure –vs- responsible disclosure



Is it legal to use a tool like this?

- Georgia Tech policies that are potentially broken by using Firesheep
 - [Computer & Network Usage and Security Policy \(CNUSP\)](#)
 - [Georgia Tech Academic Honor Code](#)
 - [Board of Regents Policy](#)



Is it legal to use a tool like this contd?

- State of Georgia laws that are potentially broken by using Firesheep
 - [Georgia Computer Systems Protection Act](#)
- U.S. Federal laws that are potentially broken by using Firesheep
 - [Computer Fraud and Abuse Act](#)
 - [Electronic Communications Privacy Act](#)



Resources

- This Presentation

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

- Trust

[http://en.wikipedia.org/wiki/Trust_\(social_sciences\)](http://en.wikipedia.org/wiki/Trust_(social_sciences))

- Risk

<http://en.wikipedia.org/wiki/Risk>



Resources contd.

- Security

<http://en.wikipedia.org/wiki/Security>

- Peer Pressure

http://en.wikipedia.org/wiki/Peer_pressure

- Oxytocin

<http://en.wikipedia.org/wiki/Oxytocin>

- Session Management

http://en.wikipedia.org/wiki/Session_management



Resources contd.

- OWASP - The Open Web Application Security Project
<https://www.owasp.org/>
- OWASP Top Ten
https://www.owasp.org/index.php/Top_Ten
- Session Hijacking
http://en.wikipedia.org/wiki/Session_hijacking



Resources contd.

- Surf Jacking

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

- Man in the middle attack (MITM)

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

- Stateless Protocol

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



Resources contd.

- HTTP Protocol

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

- HTTPS Protocol

http://en.wikipedia.org/wiki/HTTP_Secure

- HTTP Cookie

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



Resources contd.

- Cookie Secure Flag

<http://enablesecurity.com/2008/08/29/setting-the-secure-flag-in-the-cookie-is-easy/>

- Slaying Firesheep (cookie management)

<http://akfpartners.com/techblog/2010/11/20/slaying-firesheep/>

- One Time Cookies

<http://smartech.gatech.edu/jspui/bitstream/1853/37000/1/GT-CS-11-04.pdf>



Resources contd.

- CookieMonster

<http://fscked.org/projects/cookiemonster/>

- Edit Cookies

<https://addons.mozilla.org/en-US/firefox/addon/edit-cookies/>

- FaceNiff

<http://faceniff.ponury.net/>

- DroidSheep

<http://code.google.com/p/droidsheep/>



Resources contd.

- FBConTroller

<http://my.opera.com/quakerdoomer/blog/fbcontroller-v3-0-facebook-control-utility-version-3-0/>

- Hamster & Ferret

<http://erratasec.blogspot.com/2009/03/hamster-20-and-ferret-20.html>

- py-cookieJsInjection

<https://github.com/diogomonica/py-cookieJsInjection/>



Resources contd.

- Facebook - Enable Browse Facebook on a secure connection (https) when possible
<http://blog.facebook.com/blog.php?post=486790652130>
- Gmail - Always use https
<http://mail.google.com/support/bin/answer.py?hl=en&ctx=mail&answer=74765>
- Twitter - login and session are https (http no longer an option)



Resources contd.

- LinkedIn - When possible, use a secure connection (https) to browse LinkedIn
http://help.linkedin.com/app/answers/detail/a_id/6021
- Firefox
<http://www.mozilla.com/>
- HTTPS Everywhere (Firefox Add-On)
<http://www.eff.org/https-everywhere/>



Resources contd.

- Force-TLS (Firefox Add-On)

<https://addons.mozilla.org/en-US/firefox/addon/force-tls/>

- ForceHTTPS (Firefox Add-On)

<https://crypto.stanford.edu/forcehttps/>

- NoScript (Firefox Add-On)

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



Resources contd.

- Use HTTPS (Chrome Plugin)

https://chrome.google.com/extensions/detail/kbk_gnojednemejclpggpnhlhlhkmfidi/

- Fidelio (Chrome Plugin)

<http://nikcub.appspot.com/posts/fidelio-a-browser-plugin-for-secure-web-browsing>

- VPN (Virtual Private Network)

http://en.wikipedia.org/wiki/Virtual_private_network



Resources contd.

- Anonymizer

<http://en.wikipedia.org/wiki/Anonymizer>

- Proxy

http://en.wikipedia.org/wiki/Proxy_server

- TOR (The Onion Routing project)

<https://www.torproject.org/>

- Want Tor to really work?

<https://www.torproject.org/download/download.html.en#warning>



Resources contd.

- JonDonym
<https://anonymous-proxy-servers.net/>
- JAP (JonDonym Anonymous Proxy)
<http://anon.inf.tu-dresden.de/>
- I2P
<http://www.i2p2.de/>
- Full Disclosure
http://en.wikipedia.org/wiki/Full_disclosure



Resources contd.

- Ethics

<http://en.wikipedia.org/wiki/Ethics>

- Legal

<http://en.wikipedia.org/wiki/Law>

- Computer & Network Usage and Security Policy (CNUSP)

http://www.oit.gatech.edu/sites/default/files/CNUSP_new.pdf



Resources contd.

- Georgia Tech Academic Honor Code
<http://www.honor.gatech.edu/plugins/content/index.php?id=9>
- Board of Regents Policy
http://www.usg.edu/policymanual/section12/policy/12.2_disruptive_behavior
- Georgia Computer Systems Protection Act
<http://www.oit.gatech.edu/georgia-computer-systems-protection-act>



Resources contd.

- Computer Fraud and Abuse Act

<http://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap47-sec1030.htm>

- Electronic Communications Privacy Act

<http://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap119.htm>



Resources contd.

- Contact

Keith R. Watson

CoC Information Security Manager

krwatson@cc.gatech.edu

(404) 385-7401