Crypto-thon!

Your mobile apps:

Who are they really talking to?

What are they revealing about you?

How can you find out?

How can you protect yourself online?

Presented: 2015-05-07

Now let's look at some apps and find out who they are talking to, and what exactly are they sending???

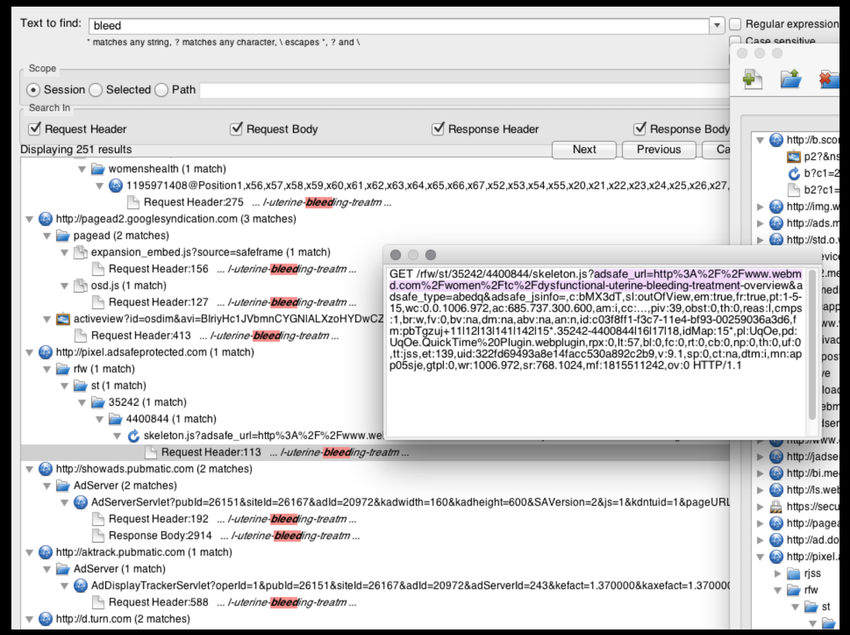
(demo goes here)

Note: this is for iPad / iOS, but the world is similar on Android, etc…

Observed: WebMD

Open App: Symptom Checker: Genitals: Bleeding: Dysfunctional Uterine Bleeding: Click on “Treatment Overview”:

Sends “dysfunctional uterine bleeding” 70+ times to non-webMD , mostly HTTP (not encrypted), to 10+ sites /advertisers / trackers, all linked to your iPad’s IP address.



"dysfunctional-uterine-bleeding" Found in reqeusts to:

http://a.postrelease.com (1 match)
http://adserve.postrelease.com (2 matches)
http://jadserve.postrelease.com (2 matches)
http://www.googletagservices.com (2 matches)
http://bi.medscape.com (1 match)
http://b.scorecardresearch.com (5 matches)
http://webmdcom.tt.omtrdc.net (5 matches)
http://pagead2.googlesyndication.com (27 matches)
http://showads.pubmatic.com (6 matches)
http://aktrack.pubmatic.com (2 matches)
http://a.collective-media.net (2 matches)
http://ib.adnxs.com (3 matches)
http://pixel.adsafeprotected.com (4 matches)
http://googleads.g.doubleclick.net (6 matches)
http://t1.gstatic.com (1 match)
http://privacy-policy.truste.com (1 match)

Observed: Kim Kardashian: Hollywood (Glu Games Inc.)

Within minutes of opening the game and beginning to play:

Ads:

11 domains

45% HTTPS(SSL)

1. http://ads.lfstmedia.com
2. http://ads.mopub.com
3. http://analytics.query.yahoo.com
4. http://apps.ad-x.co.uk
5. http://cdn.lfstmedia.com
6. http://googleads.g.doubleclick.net
7. https://apps.ad-x.co.uk
8. https://api.nanigans.com
9. https://events3.adcolony.com
10. https://events3alt.adcolony.com
11. https://mraidjs.adtilt.com

Trackers / Analytics / Behavioral Profiling:

15 domains, 53% HTTPS(SSL)

1. http://api2.playhaven.com
2. http://api.geo.kontagent.net
3. http://flurry.cachefly.net
4. http://mobile-api.geo.kontagent.net
5. http://s1.2mdn.net
6. http://tags.bkrtx.com
7. http://tags.bluekai.comhttps://adlog.flurry.com
8. https://ads.flurry.com
9. https://data.flurry.com
10. https://engine.sponsorpay.com
11. https://iosads24.adcolony.com
12. https://live.chartboost.com
13. https://marketing-ssl.upsight-api.com
14. https://sb.scorecardresearch.com
15. https://service.sponsorpay.com

App Content:

11 domains

53% HTTPS(SSL)

1. http://bid.g.doubleclick.net
2. http://code.jquery.com
3. http://d3v1lb83psg9di.cloudfront.net
4. http://engdev.geosvs.gluops.com:8025
5. http://wpc.250f.edgecastcdn.net
6. https://configuration.apple.com
7. https://cognito-identity.us-east-1.amazonaws.com
8. https://glumobile.helpshift.com
9. https://kinesis.us-east-1.amazonaws.com
10. https://sts.amazonaws.com
11. https://us-ore-00001.s3.amazonaws.com

Observed: Weight Watchers

Before even agreeing to the Application Agreement at the start you're already sending info to 2o7.net in the clear (HTTP, not HTTPS):

http://wwatchtrkappus.112.2o7.net/b/ss/wwatchtrkappus/0/OIP-4.0.0/s13698576?AQB=1&ndh=1&t=00%2F00%2F0000%2000%3A00%3A00%200%20420&c.&a.&AppID=WW%20Mobile%203.6.4%20%283.6.4.1%29&CarrierName=AT26T&LaunchEvent=LaunchEvent&DaysSinceLastUse=0&DayOfWeek=4&HourOfDay=18&Launches=2&DaysSinceFirstUse=0&DeviceName=iPad3%2C2&internalaction=Lifecycle&Resolution=2048x1536&OSVersion=iOS208.3&PrevSessionLength=5&.a&.c&ts=1430962412&aid=2AA5606B05011DC9-6000011580002A11&ce=UTF-8&pe=lnk_o&pageName=WW%20Mobile%2F3.6.4.1&pev2=ADBINTERNAL%3ALifecycle&AQE=1

including:

CarrierName AT&T - DaysSinceLastUse 0 - DayOfWeek 4 - HourOfDay 18 - Launches 2
DaysSinceFirstUse 0 - DeviceName iPad3,2

Put another way: The second you open the app, it tells 2o7.net that you're using Weight Watchers (e.g. you're on a diet), how long it's been since you last used it (did you cheat?), how often you use it, what kind of device you have…

Observed: "Good Apps": Smurf Life (Beeline Interactive)

- Doesn't collect personal information, so nothing private to send.
- One marketing tracker (fiksu.com): to be expected, but at least it's SSL (HTTPS)
- One app usage tracker (crittercism.com): to be expected, but SSL (HTTPS)
- Content sent in the clear (HTTP), but only reveals WHAT you are doing in the game
- Kids Apps are generally safter in the US because of COPPA (coppa.org)
  - FTC's Childrens' Online Privacy Protection Act, enacted 1998
  - Strong protections for "Websites that are collecting information from children under the age of thirteen"
  - There are still bad actors.
  - iOS is better than Android at weeding out bad Kids' apps

Observed: Research Notes and Other Apps…

- Apple Store doesn't work with Charles SSL Root Cert: +1 Apple!
- Chase Banking app doesn't work with Charles SSL Root Cert: +1 Chase!
  - Chase does use Splunk for tracking usage, which is to be expected
- New York Times App: Pretty good, mostly SSL (HTTPS), some still HTTP
  - App is storing time usage, where in the app users are, subscription status, etc
  - Some 3rd party analytics/trackers SSL (https://localytics.com)
  - Unfortunately, some 3rd parties NOT SSL (http://scorecardresarch.com)
  - Doubleclick (Google) Ads, but at least their SSL (HTTPS)
- Uber: Everything is encrypted with SSL (HTTPS)
- Tinder: Everything is encrypted with SSL (HTTPS) and goes to Tinder or Facebook
- Match.com: Open App: 8 different companies get notified:

  match.com, liftoff.io, urbanairship.com, crashlytics.com, ad-x.co.uk, mobileapptracking.com, apple.com

ASSUME YOU ARE BEING WATCHED

- Most apps use some combination of 3rd parties for content delivery, behavioral tracking, usage analytics, user research, A/B testing, crash reports, and advertising, so assume every app you have is. That information can be linked together with your IP Address.
- BETTER apps use only HTTPS connections. But most apps still use HTTP
- You can't stop an app from talking, but you can find out who it is talking to

- Recommendations:

1. Assume Apps are watching you and reporting to 3rd parties.

2. Don't do anything in an app you don't want to be used against you.

3. Look at what an app is sending and to who with a proxy server before giving it private or sensitive information.

HOW TOs

HOW TO: Browse Securely Online

Commercial Anonymizing VPNs:

- Route your traffic online through their servers, hiding your IP address
- Cost Money
- You have to trust the Company
- Many VPN Companies to choose from:

F-Secure.com, anonymizer.com, IVPN.net, cryptocloud.com, anonine.com, prq.se, privacy.io, …

Free Onion Routing Networks

- Route your traffic through network machines provided by fellow users
- Free (as in beer), You should donate
- You have to trust the network
- Popular Onion Networks:

Tor: torproject.org

I2P: geti2p.net

Freenet: freenetproject.org

MOST SECURE: Use many together at the same time (VERY slow)

HOW TO: Search Securely Online

HARD. There's no great solution.

- **NOT PRIVATE:** Google, Bing, Yahoo. They collect and store your search history, linking to your computer's IP, even if you have cookies turned off.

- **BETTER:** "Private" search engines: DuckDuckGo.com, StartPage.com, IXquick.com, …
  - You have to trust the Company
  - They usually do the search on Google for you (so maybe not so "private" after all)
  - Your search terms are saved on servers (e.g. "Jane Doe TERRORIST with AIDS")
  - Your IP is still sent (although many claim not to save or log that, they still get it)

- **EVEN BETTER:** Use a "Private" search engine over an encrypted VPN / Onion Network

Avoid Search Fingerprints: Your Name + Personal Info

HOW TO: Privately Use Mobile Apps

Currently (nearly) Impossible.

- Mobile Apps are new, mobile devices are harder to control, it's all very complicated.
- Even if you turn off your network (airplane mode), many apps will just send info the next time you are on the network.

Use a Proxy Server To Find out:

Who your apps are talking to

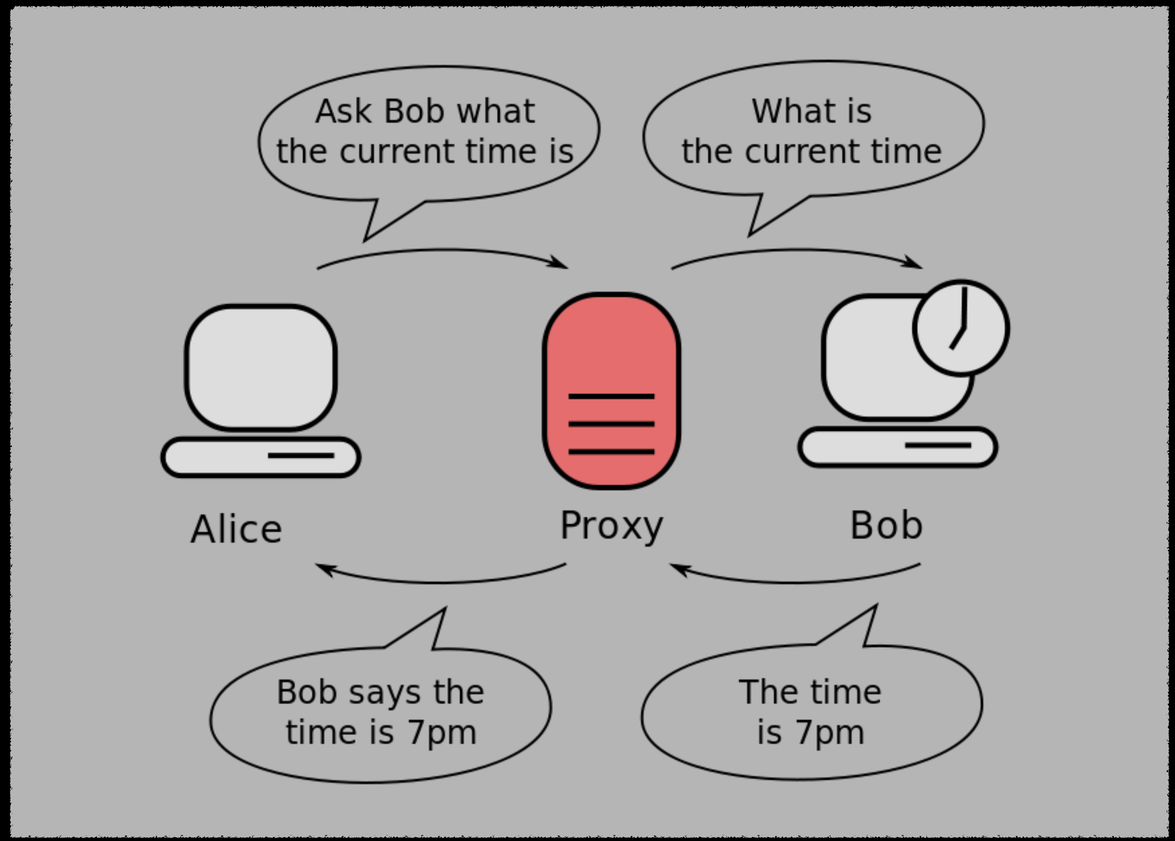
What they are telling 3rd parties about you

(It's actually not that hard…)

Watching Apps with a Proxy Server

What is a Proxy Server?

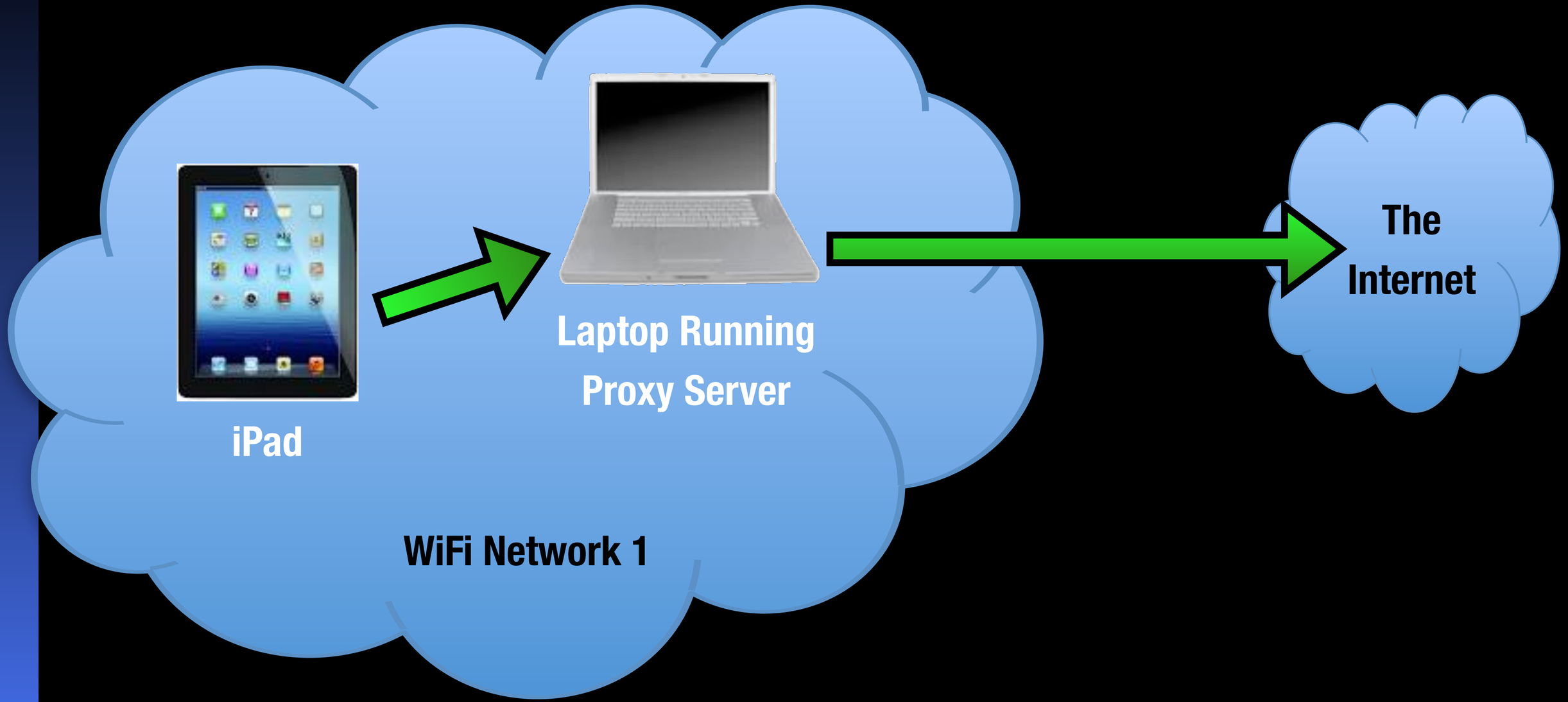
In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.



Definition and Image courtesy of Wikipedia: https://en.wikipedia.org/wiki/Proxy_server

Proxy Server: Type 1 (same WiFi)

You can configure your proxy server on the same network:



Proxy Server: Type 2 (Bridging Between Networks)

You can configure your proxy server to bridge between 2 networks:

iPad

WiFi Network 1

Laptop Running Proxy Server

Network 2

The Internet

Connected via:

Ethernet Cable

A second WiFi (e.g. $10 USB WiFi adapter)

Proxy Server: Just one problem: SSL

Proxy Servers cannot break SSL by default. (This is a good thing.)

This means you can see what server an app is talking to,

but cannot see the content of SSL (HTTPS) connections.

You can employ a "Man-in-the-Middle" attack to let the Proxy Server

decrypt and see the content of your SSL (HTTPS) communications.

This usually requires installing a "root cert" on your device.

Proxy Server Options

MANY. Lots of options to choose from from Free to Cost.

- **FREE OPTIONS: Many exist, but tend to be complicated to set up and use.**

  Fiddler is one popular one for Windows, I've never used it: telerik.com/fiddler

- **For-Cost Options: Many to choose from. Here's one I use on Mac:**

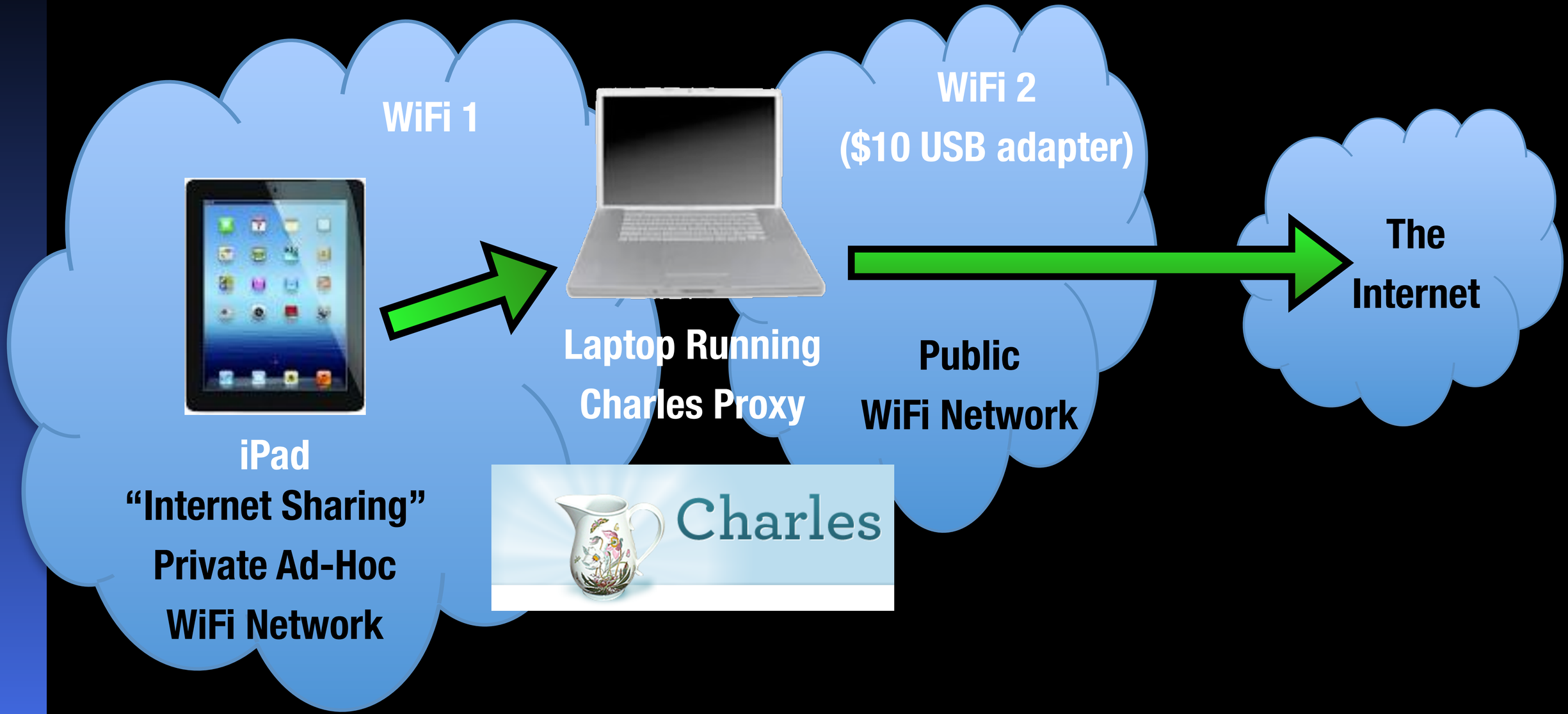
  Charles Proxy - www.charlesproxy.com - $50

  I like Charles because it is simple to use and makes it

  easy to set up"Man-in-the-Middle" attacks to open up SSL (HTTPS) connections

Proxy Server: My Setup

Charles Proxy between Ad-Hoc “Internet Sharing” Private Network and WiFi



Proxy Server HOWTO: Setting up Charles Proxy and iPad

Find Instructions Online by searching for: "charles proxy ssl ipad"

1. Computer: download and install Charles Proxy (charlesproxy.com)

3. Network: Make sure computer and iPad are on the same network

5. iPad: Go to Settings > WiFi, click on the blue "(i)" on the right for the network to change the advanced settings, scroll down, choose "Manual" for HTTP proxy, and add the IP of your laptop and the port for Charles Proxy (usually port 8888).

7. SSL: Accept the Charles Root Cert on your iPad by opening Safari, and going to:

http://charlesproxy.com/charles.crt

WARNING: YOUR IPAD IS NOW LESS SECURE (see next slide…)

WARNING: SSL Root Cert: Your iPad is Not Secure!

Your iPad is now configured to accept Charles Proxy's Root Cert

This means any site using the Charles Proxy Root Cert can "Fake" SSL Traffic from other sites. The risk is low, but still: This is a Security Risk

To Fix: Delete the Charles Root Cert from your iPad after testing:

1. Settings > General, scroll to the bottom, choose "Profiles"
2. Select the Charles Profile, choose "Delete Profile"

Do this immediately after testing! You have been warned.

Final Reminder: ASSUME YOU ARE BEING WATCHED

- Most apps use some combination of 3rd parties for content delivery, behavioral tracking, usage analytics, user research, A/B testing, crash reports, and advertising, so assume every app you have is. That information can be linked together with your IP Address.
- BETTER apps use only HTTPS connections. But most apps still use HTTP
- You can't stop an app from talking, but you can find out who it is talking to

- Recommendations:

1. Assume Apps are watching you and reporting to 3rd parties.

2. Don't do anything in an app you don't want to be used against you.

3. Look at what an app is sending and to who with a proxy server before giving it private or sensitive information.

Crypto-thon!

Your mobile apps:

Who are they really talking to?

What are they revealing about you?

How can you find out?

How can you protect yourself online?

Presented: 2015-05-07