



Web Tracking for You

Gregory Fleischer



black hat
USA 2012

INTRODUCTION

Me

Gregory Fleischer

Senior Security Consultant at FishNet Security



Disclaimer

- Why do you hate _____?



dave dave photo1dave@hotmail.com

Mar 10



to me ▾

Hello Gregory,

I am looking to find a script that can get a user's real IP address from a .onion site. Would you have anything that you can share with me. I am hope you can help on this request

Thank you very much for you help,

dave

Reasons For Tracking

- Traditional reasons for tracking web users
 - Metrics and analytics
 - Behavioral advertising and traffic monetization
 - Security mechanisms to identify legitimate users
- Monitor “malicious” users
 - Bad actors
 - Attackers
- Search for suspicious behavior

Types of Tracking

- First Party
 - Web sites you visit directly
- Third Party
 - Advertisers
 - Social network integration
- Analytics
 - Counting is not tracking?
- Tracking is pervasive



black hat
USA 2012

DEMO: COLLUSION FOR CHROME

Alternative Ways of Tracking

- Traffic inspection
 - Look at the requests
 - Local network gateway and proxies
 - Provider and host ISP levels
- Content modification
 - Modify the responses
 - Advertising injection and rewriting
 - Web bug and tracking code insertion

Key Tracking Concepts

- Fingerprinting
- Tracking
- Unmasking
- These are not mutually exclusive
 - Information from each type can reinforce others
 - Discrepancies can be correlated



black hat
USA 2012

FINGERPRINTING

Goals of Fingerprinting

- Calculate a unique fingerprint based on the user's browser and OS characteristics
- Can be more resilient to explicit privacy actions taken by users
 - Private browsing mode
 - Cookie and cache clearing

Fingerprinting Types

- Passive
- Active
- Varies based on if plugins are installed and/or enabled

Passive Fingerprinting

- Information is captured passively
- Default data automatically sent that can be used to group users into broad categories
- Functions without needed to execute JavaScript or plugin content
- However, information is easily faked or obscured

Passive Fingerprinting Data

- User-agent string and order of request headers
- Browser feature-sets and content type support
 - Anonymous FTP username
 - CSP (Content Site Policy)
 - Image types, CSS, SVG, etc.
- HTTPS handshake
 - Cipher suites and supported extensions
 - Timestamp from client machine

Passive Fingerprinting with Plugins

- Plugins may expose additional information
- Can reference content just by loading it
- Hosting site can track requests
- Plugins can include custom request header data
 - Mozilla/4.0 (Linux 2.6.38-8-generic) Java/1.7.0_05
 - X-Flash-Version: 11,3,370,178

Active Fingerprinting

- Information is actively gathered from browser using JavaScript and CSS
- Harder to fake or hide because of direct interaction
- Use feature set detection, not just based on reported browser user-agent

Active Fingerprint Data

- Standard items
 - Navigator information and screen resolution
 - Date and timezone
 - Installed plugins and fonts
- Detecting browser extensions
 - Resource references
 - Custom types



black hat
USA 2012

DEMO: CUSTOM RESOURCE DETECTION

Active Fingerprinting with Plugins

- Many plugins expose their own additional API interface to JavaScript
- Plugins can be used to access:
 - Detailed system information
 - Fonts
 - Other installed plugins
- Example:
 - Adobe Acrobat PDF plugin can enumerate printers



black hat
USA 2012

DEMO: ACTIVE PLUGIN FINGERPRINTING



black hat
USA 2012

TRACKING

Goals of Tracking

- Install a persistent tracking ID that can be used to correlate user activity
- Real world limitations require flexibility
 - Should be compact, but verifiable
 - Can be correlated
 - Doesn't always have to be transmitted or received with every request
 - Ideally, redundancy across different storage types

Web Browser Cookies

- Basic method implemented in every browser
- Browser cookie types:
 - First-party
 - “Second-party”
 - set by page dynamically
 - Third-party
- Limitations of browsers and privacy restrictions

HTML5 Storage

- Modern browsers offer divergent support across several APIs
 - localStorage
 - IndexedDB
 - FileSystem API
- Characteristics impact suitability for tracking
 - Does user have to opt-in?
 - How long does storage last?

Browser Cache

- Use embedded identifiers in cached content
- ETag references to track and correlate content
- Complicated approaches are fragile and often redundant
 - Complex request sequences
 - Redirect caching
 - Embedded basic auth references

Plugin Dependent Storage

- Plugin dependent storage methods offer flexibility
- Improvements over web browser methods
 - Usually cross-browser
 - Some are not integrated with browser private modes
 - May be harder for user to detect

Flash

- Flash Shared Objects
 - Local shared object (LSO)
 - Remote shared object
- Integrated with private browsing modes
- Cross-browser support is diverging
 - `~/.macromedia/Flash_Player/#SharedObjects/`
 - `~/.config/google-chrome/Default/Pepper Data/Shockwave Flash/WritableRoot/#SharedObjects/`



black hat
USA 2012

DEMO: FLASH REMOTE SHARED OBJECTS

Silverlight

- Silverlight exposes Isolated Storage
 - Limited quota size
- Integrated with private browsing modes
- Most XAP loading use browser cache
 - Some ability to embed resources streams
 - Satellites and on-demand loading offer little benefit
- Decent cross-browser when available

Java

- Java implements its own download cache
- Resource items and applets are cacheable
- Applets can read embedded resource streams
- Not integrated with private browsing modes
- Usually excellent cross-browser support
 - When Java works ...

Java Failures

The image shows a screenshot of an Internet Explorer browser window titled "test java tracker" with the address bar showing "http://demohost.localdomain/test-java-tracker.html". A "Java(TM) Plug-in Fatal Error" dialog box is displayed, stating: "The Java Runtime Environment cannot be loaded from <C:\PROGRA~1\Oracle\JAVAFX~1.1RU\bin\server\jvm.dll>". An "Internet Explorer Security" warning dialog is also shown, indicating that a website wants to open web content using the Java(TM) SE Runtime Environment 7 U... program. The security dialog provides details about the program's name and publisher (Oracle America, Inc.) and offers "Allow" and "Don't allow" options. Below the browser window, a yellow notification bar states "Java needs your permission to run." with buttons for "Run this time" and "Always run on this site".



black hat
USA 2012

DEMO: JAVA PERSISTENT TRACKING

Adobe Acrobat

- Adobe Acrobat Reader plugin
- `setPersistent()` function can be used for limited storage of global name/value data
- Some integration with private browsing modes
- Questionable cross-browser support
- Browsers are moving to native PDF display



black hat
USA 2012

**DEMO:
ADOBE READER PDF TRACKING**

Other Storage

- UserData
 - Internet Explorer specific
- Web SQL Database
 - SQL database exposed to browser
 - Standard abandoned, but still may be available



black hat
USA 2012

UNMASKING

Goals of Unmasking

- Identify web user's originating IP, network environment, and operating identity
- Some users attempt to obscure their true origins
 - Network proxies
 - VPN tunnels
- Determine originating user IP address
 - Force direct connection using any available mechanism
 - Correlate with additional GeoIP information

Detecting Proxy Usage

- Detect known proxies if possible
 - e.g., Tor using TorDNSExitList tools
- Generate requests and examine responses to detect differences
- Request “magic” urls to detect any local network or browser proxy
- Send requests using XMLHttpRequest or WebSocket and examine responses



black hat
USA 2012

DEMO: PROXY DETECTION

Proxy Bypasses

- Abuse browser functionality to bypass proxy
 - Use resources that may not be properly proxied
 - FTP and alternative browser requests
- In CGI style proxy, all content must be rewritten
- Some requests may be launched by browser
 - e.g., Content Site Policy (“CSP”) violation reports

Plugins and Proxies

- Various plugins can be made to leak information
- DNS leakage through unproxied UDP traffic
- Media requests may not respect host machine proxy settings
- Plugin may support direct method of communication that bypasses proxy
 - Requests that explicitly exclude proxy
 - Binary socket protocols



black hat
USA 2012

DEMO: FLASH RTMP: CONNECTION

More Aggressive Approaches

- Use sparingly, because appear overtly malicious
- Injectable content that violates user privacy
 - Capture text changes, keystrokes, images and HTML
 - Monitor clicks and likes on social network badges
 - History stealing and forced navigation
 - Abuse “trust” site status
 - Port scanning local machine and local network
 - Embed additional exploits



black hat
USA 2012

COMPLICATIONS

Private Browsing Modes

- Modern browsers have a private browsing mode
 - Cookies should not be persisted
 - Content not read from or stored in existing cache
- How to defeat?
 - If possible, correlate cookie and page contents when switching from one to the other
 - Use plugin support to enable cross-browser communications and cross reference values



black hat
USA 2012

DEMO: SAFARI PRIVATE BROWSING



black hat
USA 2012

DEMO: LOCAL CONNECTIONS

Tracking Protection Lists

- Internet Explorer implements Tracking Protection Lists (TPL)
 - Curated blacklists maintained by third-parties
 - Restricts content loaded on page
- How to defeat?
 - Manually navigate browser to content
 - Use plugins to load from blocked locations



black hat
USA 2012

DEMO: IE TRACKING PROTECTION LISTS

Third Party Cookie Restrictions

- Browser can block or restrict third-party cookies
 - Safari has default blocking (limited to visited sites)
 - Internet Explorer, Firefox and others are opt-in
- How to defeat?
 - Use known workarounds to simulate user interactions
 - Cross-domain postMessage support to pass cookies between coordinating sites and store in localStorage



DEMO: LOCAL STORAGE AND POSTMESSAGE

Do Not Track

- Do Not Track (DNT)
- Optional, sent as browser HTTP request header
 - “Opt-in” signal to third parties not to track
 - Think of it as the “Don’t Track Me Bro” header
- How to defeat?
 - Do nothing (or point and laugh)
 - Use protocols that aren’t HTTP (e.g., FTP, binary sockets) if technical restrictions ever enforced



black hat
USA 2012

TRACKING SERVER

Goals of Tracking Server

- Create suitable environment to track web users
- Approach is to be as “insecure” and open as possible
 - Support insecure protocols
 - Allow all cross-domain requests
- Use separate domain, third-party location
- Bootstrap from first-party content if needed

Existing Sites

- BrowserSpy (<http://browserspy.dk/>)
- Panopticklick (<https://panopticklick.eff.org/>)
- Cross-browser fingerprinting test 2.0 (<http://fingerprint.pet-portal.eu/>)
- Evercookie (<http://samy.pl/evercookie/>)
- Metasploit Decloaking engine (<http://decloak.net/>)
- IP Check (<http://ip-check.info/>)

Existing Site Shortcomings

- Existing sites offer disjointed functionality
- Need purpose built tools to address weaknesses
 - Interaction with an untrusted third-party site
 - Storage in unknown locations and formats
 - Lack of comprehensiveness
- Some features little more than proof-of-concept
 - Big difference between displaying and storing
 - Integration capabilities missing or non-existent

Design Goals

- Design with correlation in mind
 - Tracking tokens are cleared over time
 - Fingerprinting may not yield unique results
- Combine and cross-reference collected data
- The larger the network view, the more effective
- Methods to inject web tracking code
 - Embed in HTML on your web site
 - Use a transparent network proxy

Protocol Support

- Tracking server should support several protocols
 - FTP
 - DNS
 - HTTP
 - HTTPS
 - Policy servers for Flash and Silverlight
 - Binary sockets
 - Media (RTMP, etc.)

Alpha Release

- Tracking server and utilities
 - Tracking server suitable for network or local machine
 - Local, transparent HTTP proxy capable of injecting tracking code
- Open Source
- Written in Python, GPLv3 license
- Download: <https://code.google.com/p/wtfy/>
- Many features missing!

Conclusions

- Final Thoughts
 - Web tracking is inevitable
 - Impractical to prevent web tracking between coordinating sites
- Questions?

Contact

- Send your feature requests and hate mail
- gfleischer@gmail.com

Feedback Forms

- Please complete the Speaker Feedback Surveys.
- This will help speakers to improve and for Black Hat to make better decisions regarding content and presenters for future events.

