Client Fingerprinting Techniques: Report Outline

Team#7: Alex Feng, Tristan Luther, Yuna Oh

Abstract

- Client fingerprinting is a tracking technique to collect information about users. This data can be used for a variety of purposes such as analytics, advertising, and fraud detection. Multiple methods exist to collect and use client data for security purposes but this added data collection also poses a potential security risk. Our demonstration shows the device fingerprinting techniques that can be employed by websites to prevent user accounts having multiple sign-ins at different locations, preventing possible fraud. Our demo also displays that sensitive user data is also being saved to servers where the possibility for it to be exploited exists.

Introduction

- Client fingerprinting is a modern security technique to verify the identity of a user connected to a server. Give more general information on fingerprinting.

Background

- Discuss client fingerprinting in the context of identifying fraud, how the two relate and use that to introduce the problem of a session hijacking attack.
- Discuss the many forms client fingerprinting can take to validate identity
- Explain the parties that would be interested in client fingerprinting solutions and what many of them do
    - Banks (logins from unknown locations require additional user verification)
    - Government Organizations/Contractors

Approach/solutions

- Show our demo and what is being collected, give a description of the backend and how user data is being collected and used to catch non-authentic session logins.
- Discuss the potential security concerns of gathering user data in this manner.
- Explain algorithm used to determine an in-authentic login.

Findings/results

- Show how simulated invalid logins are caught and logged into the database.

Discussion

- Weekly meetings at Friday 1-2pm
- Discuss plans, current progress, work on project assignments
    - Goals
    - Research plans
    - Structure of project
    - Data flow
    - Algorithm for determining whether a new user (unrecognized user) has signed in
    - Technologies used
    - Programming languages used
    - Presentation flow

Team and contributions

- Alex
    - Design login pages

    - Setup login
    - Gather device info (e.g. OS, device specifics, version, timezone)

- Tristan
    - Client Data Interface Layout (website)
    - Location based fingerprinting research/implementation
    - General Presentation Research

- Yuna
    - Design Home Page
    - Research/Implementation logic for New login notification
    - Web development Research / Combine Sites

Conclusion

- Reiterate the results of the demo and contrast how this data could validate identity while also preventing session hijacking attacks.
- Provide some resources to the reader to implement client fingerprinting techniques of web servers that they may manage.
    - http://clientjs.org/