Automated Black-Box Detection of Side-Channel Vulnerabilities in Web Applications

Peter Chapman
David Evans
University of Virginia
http://www.cs.virginia.edu/sca/

CCS '11
October 19, 2011
Side-Channel Leaks in Web Apps

HTTPS over WPA2

Chen⁺, Oakland 2010
Modern Web Apps

Dynamic and Responsive Browsing Experience

On-Demand Content

- Traffic
- Latency
- Responsiveness

Traffic is now closely associated with the demanded content.
Motivation: Detect Vulnerabilities
Motivation: Evaluate Defenses

Randomized or Uniform Communication Attributes

Packet Sizes

Transfer Control Flow

Requests and Responses

Inter-Packet Timings

HTTPoS [Luo+, NDSS 2011]
Approach

Attacker Builds a Classifier to Identify State Transitions
A Black-Box Approach

Similar to Real Attack Scenario

Applicable to Most Web Applications

HTTPS over WPA2

Full Browser Analysis
Black-Box Web Application Crawling
Crawljax

Web crawling back-end drives Firefox instance via Selenium

Designed to build Finite-State Machines of AJAX Applications

http://crawljax.com/
Approach
Threat Models and Assumptions

Both: Victim begins at root of application

**WiFi**
No disruptive traffic
Distinguish incoming and outgoing

**ISP**
Access to TCP header
Nearest-Centroid Classifier

Given an unknown network trace, we want to determine to which state transition it belongs.

Classify unknown trace as one with the closest centroid.
Distance Metrics

Metrics to determine similarity between two traces

Edit-Distance
Unweighted edit distance

Size-Weighted-Edit-Distance
Convert to string, weighted edit distance based on size

192.168.1 -> 72.14.204 62 bytes
72.14.204 -> 192.168.1 62 bytes

72.14.204 -> 192.168.1 482 bytes
192.168.1 -> 72.14.204 693 bytes

192.168.1 -> 72.14.204 62 bytes
72.14.204 -> 192.168.1 62 bytes

192.168.1 -> 72.14.204 281 bytes
72.14.204 -> 192.168.1 1860 bytes

192.168.1 -> 72.14.204 453 bytes
72.14.204 -> 192.168.1 2828 bytes
Classifier Performance – Google Search

First character typed, ISP threat model

Accuracy

Total-Source-Destination, Size-Weighted-Edit-Distance

Random, Edit-Distance

Matches
Quantifying Leaks

Leak quantification should be independent of a specific classifier implementation.
Entropy Measurements

Entropy measurements are a function of the average size of an attacker's uncertainty set given a network trace.

Problems
The same network trace can be the result of multiple classifications.
Every possible network trace is unknown.

Traditional Entropy Measurement:

\[ H(X) = \sum_{i=0}^{n} \log_2 p(\bar{x}_i) \]

- Size of uncertainty set
- Centroid for class
- Use the centroids
- Number of classes

Traditional Entropy Measurement
Determining Indistinguishability

At what point are two classes indistinguishable (same uncertainty sets)?
Determining Indistinguishability

Compare points to centroids?

Same issue with individual points.

In practice the area can be very large due to high variance in network conditions.
Entropy Distinguishability Threshold

Threshold of 75%
# Google Search Entropy Calculations

Desired metrics are calculated for different thresholds (100%, 75%, and 50%). These metrics are:

- **Total-Source-Destination**
- **Size-Weighted-Edit-Distance**
- **Edit-Distance**

The values are measured in bits of entropy:

<table>
<thead>
<tr>
<th>Metric</th>
<th>100%</th>
<th>75%</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired</td>
<td>4.70</td>
<td>4.70</td>
<td>4.70</td>
</tr>
<tr>
<td>Total-Source-Destination</td>
<td>2.95</td>
<td>2.40</td>
<td>0.44</td>
</tr>
<tr>
<td>Size-Weighted-Edit-Distance</td>
<td>1.13</td>
<td>0.56</td>
<td>0.44</td>
</tr>
<tr>
<td>Edit-Distance</td>
<td>4.70</td>
<td>4.70</td>
<td>4.70</td>
</tr>
</tbody>
</table>

*(measured in bits of entropy)*

We'd rather not use something with an arbitrary parameter.
Fisher Criterion

Fisher Criterion

Marred Arthur Guinness' daughter, secret wedding (she was 17) in 1917

Ronald Fisher (1890-1962)

Developed many statistical tools as a part of his prominent role in the eugenics community

Arthur Guinness (1835-1910)
Fisher Criterion

Like all good stories, this one starts with a Guinness.

Arthur Guinness (1725-1803)  “Guinness is Good for You”
Fisher Criterion

\[ F(X) = \frac{\sigma^2_{\text{between}}}{\sigma^2_{\text{within}}} = \frac{\sum_{i=0}^{n} m \cdot (\bar{x}_i - \bar{x})^2}{\sum_{r} \sum_{j} \sum_{i=0}^{m} (\bar{x}_i - \bar{x}_j)^2} \]

\[ F(X) = 11 \]

\[ F(X) = 0 \]
# Google Search Fisher Calculations

## Fisher Criterion Calculations

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total-Source-Destination</td>
<td>4.13</td>
</tr>
<tr>
<td>Size-Weighted-Edit-Distance</td>
<td>41.7</td>
</tr>
<tr>
<td>Edit-Distance</td>
<td>0.00</td>
</tr>
</tbody>
</table>

## Entropy Calculations

<table>
<thead>
<tr>
<th></th>
<th>100%</th>
<th>75%</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Desired</strong></td>
<td>4.70</td>
<td>4.70</td>
<td>4.70</td>
</tr>
<tr>
<td><strong>Total-Source-Destination</strong></td>
<td>2.95</td>
<td>2.40</td>
<td>0.44</td>
</tr>
<tr>
<td><strong>Size-Weighted-Edit-Distance</strong></td>
<td>1.13</td>
<td>0.56</td>
<td>0.44</td>
</tr>
<tr>
<td><strong>Edit-Distance</strong></td>
<td>4.70</td>
<td>4.70</td>
<td>4.70</td>
</tr>
</tbody>
</table>
Other Applications

Bing Search Suggestions

Yahoo Search Suggestions
Other Applications

NHS Symptom Checker

Find your symptom checker

1 Introduction  2 Who is the checker for?

Please select the general area of your symptom:

- Rashes or skin problems [Help]
- Pregnancy problems [Help]
- Accident, wound or injury [Help]
- Stomach, bowel and bladder [Help]
- Head and neck [Help]
- General health [Help]
- Bones and muscles [Help]
- Children's health [Help]
- Ear, nose and throat [Help]

See paper for Google Health Find-A-Doctor
Evaluating Defenses

With black-box approach, evaluating defenses is easy!

HTTPOS: Sealing Information Leaks with Browser-side Obfuscation of Encrypted Flows

Xiapu Luo§*, Peng Zhou§, Edmond W. W. Chan§, Wenke Lee†, Rocky K. C. Chang§, Roberto Perdisci‡
The Hong Kong Polytechnic University§, Georgia Institute of Technology†, University of Georgia‡
{csxluo, cspzhouroc, cswwchan, csrchang}@comp.polyu.edu.hk, wenke@cc.gatech.edu, perdisci@cs.uga.edu

Abstract

Leakage of private information from web applications—even when the traffic is encrypted—is a major security threat to many applications that use HTTP for data delivery. A common approach to preventing leaks is to obfuscate the encrypted traffic by changing the statistical features of traffic flows, e.g., packet size and packet timing information. Existing methods for defending against information leakage attacks do not work well when the statistical signatures of the encrypted flows can be profiled from traffic features [29]. HTTPOS addresses this problem by using an obfuscation technique that hides traffic features that can be profiled.
# HTTPOS Search Suggestions

### Before HTTPOS

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random</td>
<td>2.9%</td>
<td>35.6%</td>
</tr>
<tr>
<td>Total-Source-Destination</td>
<td>46.1%</td>
<td>100%</td>
</tr>
<tr>
<td>Size-Weighted-Edit-Distance</td>
<td>46.1%</td>
<td>100%</td>
</tr>
<tr>
<td>Edit-Distance</td>
<td>3.8%</td>
<td>39.5%</td>
</tr>
</tbody>
</table>

### After HTTPOS

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random</td>
<td>2.9%</td>
<td>35.6%</td>
</tr>
<tr>
<td>Total-Source-Destination</td>
<td>3.4%</td>
<td>38.0%</td>
</tr>
<tr>
<td>Size-Weighted-Edit-Distance</td>
<td>3.8%</td>
<td>38.0%</td>
</tr>
<tr>
<td>Edit-Distance</td>
<td>3.4%</td>
<td>35.5%</td>
</tr>
</tbody>
</table>
# HTTPPOS Search Suggestions

## Before HTTPPOS

<table>
<thead>
<tr>
<th>Fisher Criterion Calculations</th>
<th>Before HTTPPOS</th>
<th>After HTTPPOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total-Source-Destination</td>
<td>4.13</td>
<td>0.28</td>
</tr>
<tr>
<td>Size-Weighted-Edit-Distance</td>
<td>41.7</td>
<td>0.43</td>
</tr>
<tr>
<td>Edit-Distance</td>
<td>0.00</td>
<td>0.14</td>
</tr>
</tbody>
</table>

HTTPPOS works well with search suggestions
### HTTP POS Google Instant

#### Before HTTP POS

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random</td>
<td>2.9%</td>
<td>35.6%</td>
</tr>
<tr>
<td>Total-Source-Destination</td>
<td>47.5%</td>
<td>88.3%</td>
</tr>
<tr>
<td>Size-Weighted-Edit-Distance</td>
<td>7.3%</td>
<td>52.6%</td>
</tr>
<tr>
<td>Edit-Distance</td>
<td>7.7%</td>
<td>56.0%</td>
</tr>
</tbody>
</table>

#### After HTTP POS

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random</td>
<td>2.9%</td>
<td>35.6%</td>
</tr>
<tr>
<td>Total-Source-Destination</td>
<td>43.7%</td>
<td>87.6%</td>
</tr>
<tr>
<td>Size-Weighted-Edit-Distance</td>
<td>8.2%</td>
<td>51.4%</td>
</tr>
<tr>
<td>Edit-Distance</td>
<td>8.7%</td>
<td>55.0%</td>
</tr>
</tbody>
</table>
### Fisher Criterion Calculations

<table>
<thead>
<tr>
<th>Before HTTPPOS</th>
<th>After HTTPPOS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fisher Criterion Calculations</strong></td>
<td><strong>Fisher Criterion Calculations</strong></td>
</tr>
<tr>
<td>Total-Source-Destination</td>
<td>1.13</td>
</tr>
<tr>
<td>Size-Weighted-Edit-Distance</td>
<td>0.34</td>
</tr>
<tr>
<td>Edit-Distance</td>
<td>0.22</td>
</tr>
</tbody>
</table>

No training phase, so HTTPPOS works well with search suggestions, but not entire pages.
Summary

Developed Fisher Criterion as an alternative measurement for information leaks in this domain.

Evaluated real web apps and a proposed defense system.


With a tutorial.