This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.
56% of global internet users “live in countries where political, social, or religious content was blocked online.” [1]
Link Obfuscation
Look-Like Something

Encryption doesn’t hide metadata [2].
Mimicry

Implementing mimicry is impractical [4].
Tunneling

Non-standard camera input is detectable [6].
To be indistinguishable to the censor, we want to...

(1) run a standard instance of a target application,
(2) with a standard input,
(3) while embedding data into the stream
Balboa is a framework which...

(1) runs an *unmodified* binary of a TLS-enabled target application,
(2) on its standard input,
(3) while manipulating its TCP stream to embed/extract covert data
or

Balboa

- Dylib Injection
- TLS Rewriter
- Traffic Model

Firefox

Linux

Cloud
Traffic Model: Internet Radio

- Encrypted TLS Record
- Ogg Page
  - Ogg Metadata
  - Vorbis Audio Data
or

Balboa

Dylib Injection

TLS Rewriter

Traffic Model

Covert Data
Dynamic Library Injection

connect(client_fd, ip, port)
write(client_fd, buffer, len) $\rightarrow$ bytes_written
read(client_fd, buffer, len) $\rightarrow$ bytes_read
Security Evaluation

Balboa only modifies data which is indistinguishable from randomness.
## Evaluation: Internet Radio

<table>
<thead>
<tr>
<th></th>
<th>VLC</th>
<th>MPlayer</th>
<th>MPV</th>
<th>Audacious</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accuracy with 5ms ± 1ms latency</strong></td>
<td>0.72 ± 0.08</td>
<td>0.50 ± 0.10</td>
<td>0.53 ± 0.09</td>
<td>0.73 ± 0.06</td>
</tr>
<tr>
<td><strong>Accuracy with 10ms ± 1ms latency</strong></td>
<td>0.67 ± 0.09</td>
<td>0.55 ± 0.10</td>
<td>0.55 ± 0.09</td>
<td>0.68 ± 0.06</td>
</tr>
</tbody>
</table>
## Evaluation: Web Browsing

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Firefox</th>
<th>Curl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsing Wikipedia</td>
<td>0.69 ± 0.01</td>
<td>0.71 ± 0.08</td>
</tr>
<tr>
<td>File Download</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy with 5ms ± 1ms latency</td>
<td>0.69 ± 0.01</td>
<td>0.71 ± 0.08</td>
</tr>
<tr>
<td>Accuracy with 10ms ± 1ms latency</td>
<td>0.66 ± 0.01</td>
<td>0.79 ± 0.08</td>
</tr>
</tbody>
</table>
Bobbing and Weaving around Network Censorship  
Marc B. Rosen, James Parker, Alex J. Malozemoff

Questions? Email us! balboa@galois.com

https://github.com/GaloisInc/balboa
https://github.com/GaloisInc/stallone
Citations


